AN ISOMORPHISM THEOREM BETWEEN THE EXTENDED GENERALIZED BALANCED TERNARY NUMBERS AND THE *P*-ADIC INTEGERS

By

WEI Z. KITTO

A DISSERTATION PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA

1991

ACKNOWLEDGEMENTS

I would like to thank my advisors, Dr. David C. Wilson and Dr. Gerhard X. Ritter, for introducing me to the exciting research area of image processing and for their insights into the process of researching. I would like to especially thank Dr. Wilson for his constant patience and encouragement.Without him this dissertation would not have been possible. I would like to thank the other members on my graduate committee, especially Dr. Andrew Vince, for all their help.

Most of all, I thank my parents and my husband for their support during the years of my graduate study.

TABLE OF CONTENTS

Abstract of Dissertation Presented to
the Graduate School of the University of Florida
in Partial Fulfillment of the Requirements for the Degree
of Doctor of Philosophy

AN ISOMORPHISM THEOREM BETWEEN
THE EXTENDED GENERALIZED BALANCED TERNARY NUMBERS
AND THE p-ADIC INTEGERS

By

Wei Zhang Kitto

December 1991

Chairman: Dr. David C. Wilson
Cochairman: Dr. Gerhard X. Ritter
Major Department: Mathematics

The Generalized Balanced Ternary Numbers (GBT) were developed by L. Gibson and D. Lucas (1982), who describe them as a hierarchical addressing system for Euclidean space that has a useful algebraic structure derived from a hierarchy of cells. At each level the cells are constructed of cells from the previous level according to a rule of aggregation. For each dimension the most basic cell is different. In dimension two it is a hexagon and in dimension three a truncated octahedron. The basic cell in dimension n is an $n+1$-permutohedron. A finite sequence of the GBT digits $0, 1, \ldots, 2^{n+1}-2$ can be used to identify any cell in n-dimensional Euclidean space. Under the addition and multiplication which are defined in a manner analogous to decimal arithmetic, the set of GBT addresses forms a commutative ring $\mathbf{GBT_n}$. The Extended Generalized Balanced Ternary ring $\mathbf{EGBT_n}$ consists

of all such infinite sequences. The primary goal of this research is to prove that if $2^{n+1} - 1$ and $n + 1$ are relatively prime, then $\mathbf{EGBT_n}$ is isomorphic as a ring to the $(2^{n+1} - 1)$- adic integers. Extensions of this result are also given. The secondary goal of this research is to discuss template decomposition and inversion over hexagonally sampled images.

CHAPTER 1

INTRODUCTION

The 2-dimensional Generalized Balanced Ternary Numbers ($\mathbf{GBT}_2$) were developed by L. Gibson and D. Lucas as a method to address a hexagonal tiling of Euclidean 2-space [6,7,8,17,18]. They describe the hexagonal tiling as a hierarchy of cells, where at each level in the hierarchy new cells are constructed according to a rule of aggregation. The most basic cell in this tiling is a hexagon. A hexagon and its six neighbors form a cell called a first level aggregate. (The first level aggregates obviously also tile 2-space and also have the uniform adjacency property that the hexagonal tiling possesses.) A first level aggregate and its six neighbors form a second level aggregate. The hierarchy continues in the obvious way. Figures 1, 2, and 3 illustrate a first, second and third level aggregate, respectively.

The $\mathbf{GBT}_2$ addressing method of the tiling above is based on the following scheme. A first level aggregate L_1 is chosen and labeled with the integers 0 through 6 as shown in Figure 4. The six first level aggregates neighboring L_1 are labeled with two digits as shown in Figure 5 and form a second level aggregate L_2; each digit is some integer from 0 to 6. Reading from right to left, the first digit corresponds to where the labeled hexagon is in its first level aggregate L_1 and the second digit corresponds to where L_1 is in the second level aggregate L_2. Figure 6 shows the labeling of the third level aggregate centered at L_1. Continuing in this manner, every hexagon in the tiling corresponds to a unique finite sequence, an address, with entries integers from 0 to 6.

Most gridded representations used in image processing use rectangular pixels corresponding to tiling the plane with squares. Reasons for interest in a hexagonal grid in image processing are that natural scenes in low resolution images look more "natural" when presented in a hexagonal rather than square grid, hexagons can be grouped into aggregates and each pixel in a hexagonal grid has six equal neighbors, thus avoiding the 4-neighbor/8-neighbor problem.

B. H. McCormick [21] in 1963 proposed the hexagonal array as a possible gridded representation for planar images. M. J. E. Golay [9] in 1969 applied the hexagonal array in a parallel computer and developed the hexagonal pattern transformation. K. Preston [22] in 1971 developed "a special purpose computer system which uses hexagonal pattern transformations to perform picture processing at high speed." D. Lucas and L. Gibson [6,7,8,17,18] in 1982 exploited the geometric advantages of the hexagonal representation in their applications to automatic target recognition. N. Ahuja [1] in 1983 investigated polygonal decomposition for such hierarchical image representations as triangular, square, and hexagonal. D. K. Scholten and S. G. Wilson [24] in 1983 showed that the hexagonal lattice outperforms the usual square lattice as a basis for performing the chain code quantization of line drawings. J. Serra [25] in 1988 discussed the properties of the hexagonal grid.

The ring $\mathbf{GBT}_2$ can be thought of as the set of all finite sequences with entries from the set $\{0,1,2,3,4,5,6\}$. One uses $\mathbf{EGBT}_2$, the 2-dimensional Extended Generalized Balanced Ternary, to denote the set of all infinite sequences with entries from the set $\{0,1,2,3,4,5,6\}$. Motivation for this dissertation originated in a question posed by D. Lucas to my cochairman G. X. Ritter. Lucas wondered if $\mathbf{EGBT}_2$ is isomorphic as a ring to the 7-adic integers. (It will be shown in Chapter 2 that EGBT_2 can be made into a ring.) The answer is that $\mathbf{EGBT}_2$ is isomorphic as a ring to the 7-adic integers and this is shown in Chapter 2.

Lucas and Gibson [6] have defined an n-dimensional Generalized Balanced Ternary ($\mathbf{GBT}_n$) ring for each $n \geq 1$ as the set of all finite sequences with entries from the set $\{0, 1, \ldots, q-1\}$, where $q = 2^{n+1} - 1$. As an addressing method, the $\mathbf{GBT}_n$ addresses an $(n+1)$-permutohedron tiling or packing of n-space. (As mentioned by Lucas [6], the permutohedrons in 2-space are hexagons; in 3-space they are truncated octahedrons.) The n-dimensional Extended Generalized Balanced Ternary Numbers $\mathbf{EGBT}_n$ are the set of all infinite sequences with entries from the set $\{0, 1, \ldots, q-1\}$, where $q = 2^{n+1} - 1$. It is natural to ask for what values of n, if any, other than 2 is the $\mathbf{EGBT}_n$ isomorphic as a ring to the q-adic integers. In fact Lucas wrote to the author posing this question [16]. In Chapter 3 it is shown that for certain values of n $\mathbf{EGBT}_n$ is isomorphic as a ring to the q-adic integers.

In Chapter 4 another proof is given of the main result in Chapter 3. The proof is due to A. Vince and is algebraic in nature.

In Chapter 5, the algebraic properties of a special linear transformation which takes the hexagonal lattice associated with $\mathbf{GBT}_2$ into itself are investigated.

In Chapter 6, the inversion and decomposition of the templates over the hexagonally sampled images are discussed.

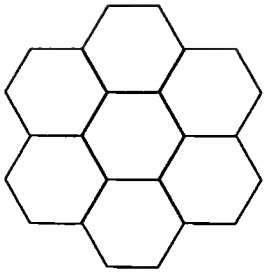


Figure 1 : The First Level Aggregate.

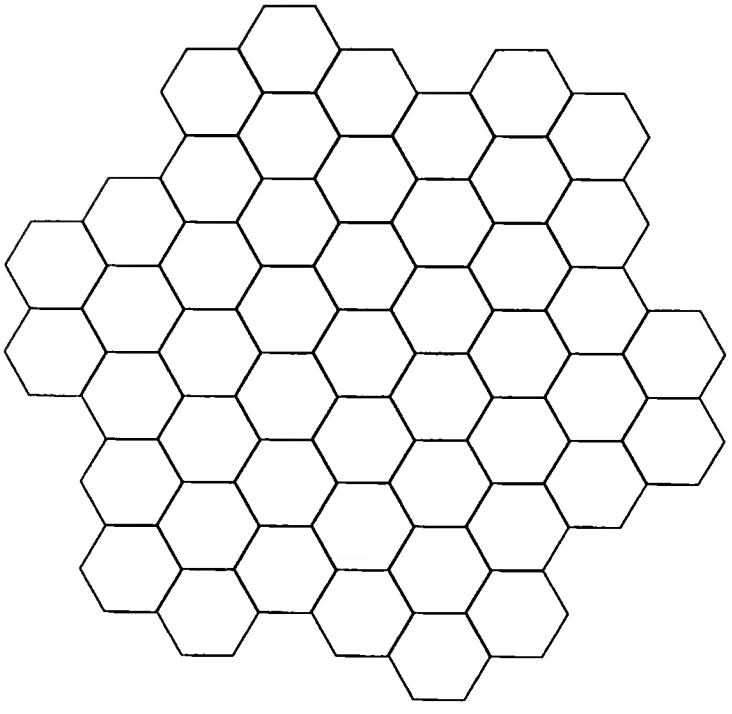


Figure 2 : The Second Level Aggregate.

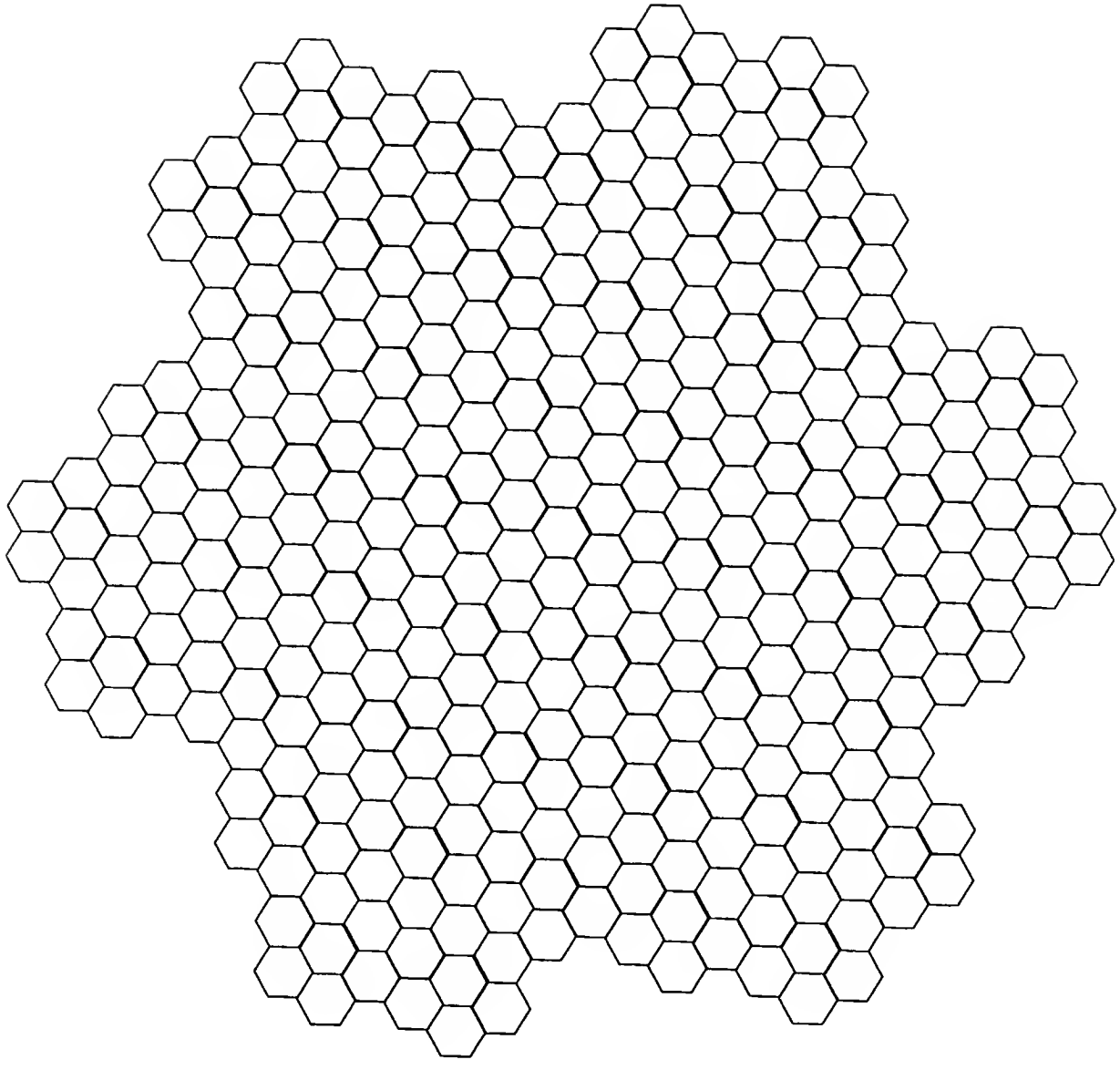


Figure 3 : The Third Level Aggregate.

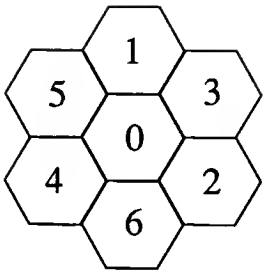


Figure 4 : The GBT Address of First Level Aggregate.

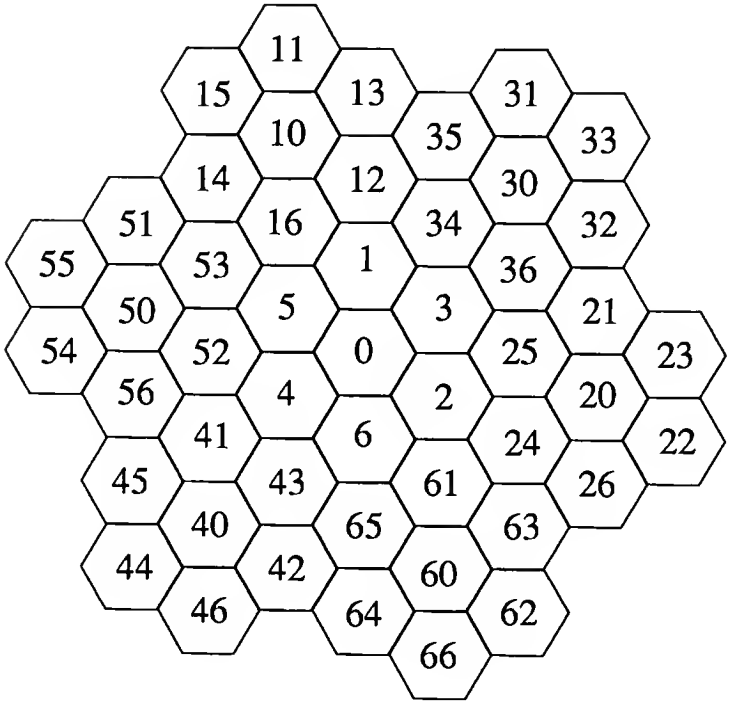


Figure 5 : The GBT Address of Second Level Aggregate.

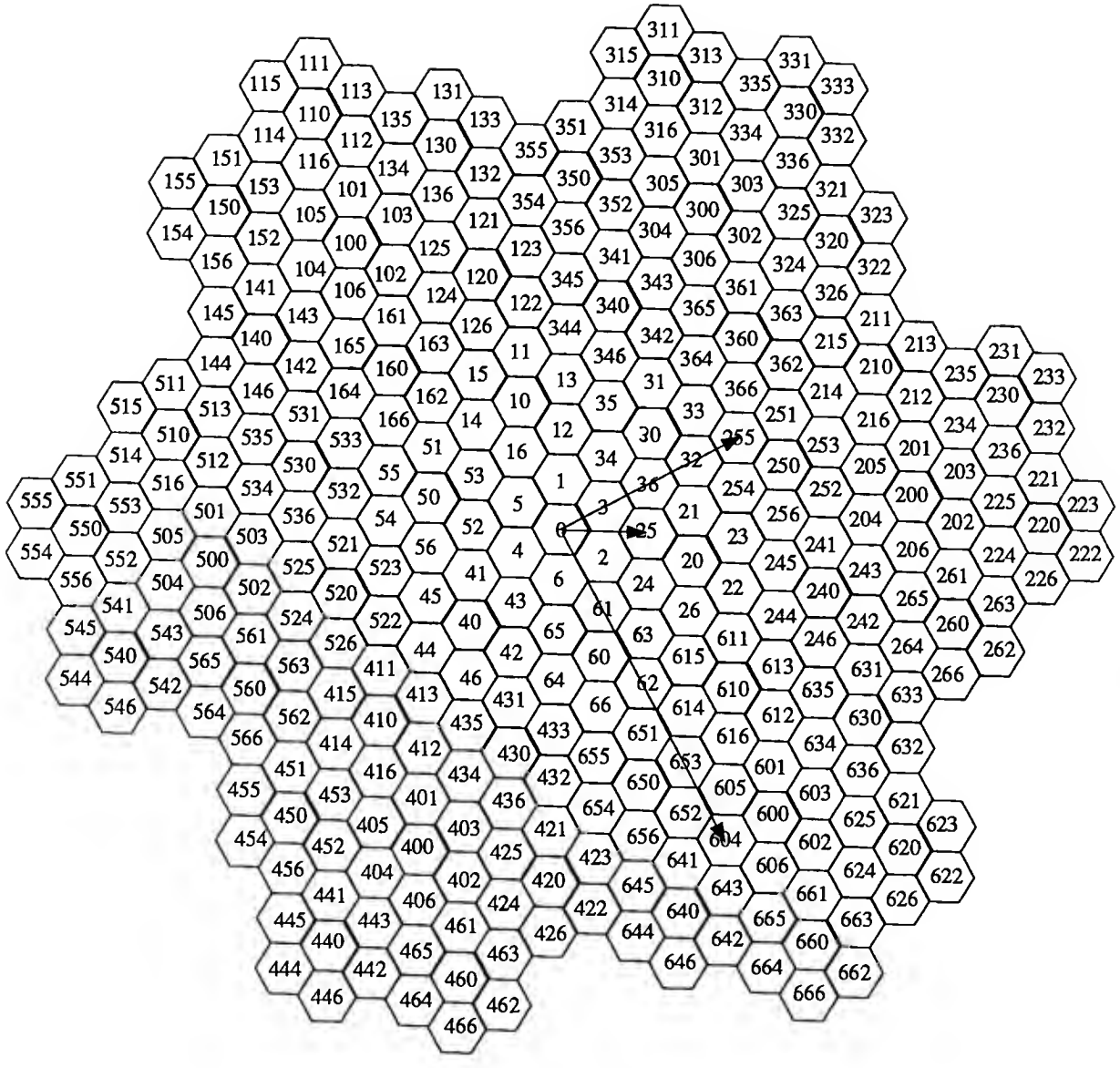


Figure 6 : The GBT product of 255 and 25 over the Third Level Aggregate.

CHAPTER 2

THE 7 – adic INTEGERS AND THE RING $\mathbf{EGBT}_2$

In this Chapter we will prove that the 7-adic and 15-adic integers are isomorphic to $\mathbf{EGBT}_2$ and $\mathbf{EGBT}_3$, respectively. These particular case studies will lead to a more general result in Chapter 3.

§2.1. Introduction

As stated in Chapter 1, one of the goals of this chapter is to prove the existence of a ring isomorphism from the 7-adic integers onto the $\mathbf{EGBT}_2$, a ring defined by an unusual remainders and carries tables.

Recall that the p-adic integers, $\mathbf{Z}_p$, can be thought of as the set of all series $a_1 + a_2p + a_3p^2 + ... + a_kp^{k-1} + ..., 0 \leq a_k < p$ where addition and multiplication are performed with the usual "carries rules" for arithmetic modulo p. Since the integer p is primarily a place holder, the elements of $\mathbf{Z}_p$ can be thought of as the set of all infinite sequences $a = (a_k) = (a_1, a_2, \ldots, a_k, \ldots)$, where $0 \leq a_k < p$. In this setting, if $a = (a_k)$ and $b = (b_k)$ are elements of $\mathbf{Z}_p$, then the sum $a + b = (s_k)$, where $a_1 + b_1 = c_2p + s_1$ and $a_k + b_k + c_k = c_{k+1}p + s_k$. Similarly, the product ab is defined by $ab = (t_k)$, where $a_1b_1 = d_2p + t_1$ and $a_1b_k + a_2b_{k-1} + ... + a_kb_1 + d_k = d_{k+1}p + t_k$. Here the variables c_k and d_k are the *carries,* and the variables s_k and t_k are the *remainders.* (These familiar carry and remainder rules are presented in Table 1.) Note that the carries are uniquely determined by the fact that each s_k and t_k is between 0 and p. Recall that the basic rules of arithmetic imply that

these addition and multiplication operations satisfy the associative, commutative, and distributive laws. Moreover, the sequence (0,0,...) is the additive zero element and the sequence (1,0,0,...) is the multiplicative identity. If p is a prime, then an element has a multiplicative inverse if and only if the first coordinate is nonzero. We use $\mathbb{Z}_7$ to denote this description of the p-adic integers for the case when $p = 7$. (The above discussion of the p-adic integers is essentially the same as the one given on page 43 of Kaplansky [11].)

Let H denote the addressed hexagonal tiling of the plane described in Chapter 1. Guided by algebraic rules associated with H, L. Gibson and D. Lucas [6,7] defined new rules for addition and multiplication of the elements in $\mathbf{EGBT}_2$, the set of all infinite sequences $a = (a_k) = (a_1, a_2, a_3, ...)$ with integer entries $0 \leq a_k \leq 6$, that makes $\mathbf{EGBT}_2$ into a ring. If a and b are elements in $\mathbf{EGBT}_2$, then define $a+b = (s_k)$ by $a_k + b_k + c_k = c_{k+1}7 + s_k$, where the rules for determining the *carries* c_k are given in Table 2, and; define $ab = (t_k)$ by $a_1b_k + ... + a_kb_1 + d_k = d_{k+1}7 + t_k$, where the *carries* d_k are given in Table 2. The rules for the remainders remain the same as in $\mathbb{Z}_7$ for both addition and multiplication. It is straightforward to show that under these operations $\mathbf{EGBT}_2$ is made into a ring. It is worth noting here that an element (a_k) has a multiplicative inverse if and only if $a_1 \neq 0$. Thus, it will be shown that $\mathbf{EGBT}_2$ with its very odd *carry rules* has the same ring structure as $\mathbb{Z}_7$ with its very familiar *carries rules*.

It is well known that $\mathbf{Z}_7$ is isomorphic to the inverse limit of the system $\{\mathbb{Z}/(7^k); k = 1, 2, \dots\}$. The fundamental idea of the proof that $\mathbf{EGBT}_2$ is isomorphic to $\mathbb{Z}_7$ is to show that if I_k is the ideal in $\mathbf{EGBT}_2$ defined by $I_k = \{(\underbrace{0, ..., 0}_{k}, x_{k+1}, x_{k+2}, ...) : x_i \in \mathbf{Z}/(7)\}$, then $\mathbf{EGBT}_2$ is isomorphic to the inverse limit of the system $\{\mathbf{EGBT}_2/I_k; k = 1, 2, \dots\}$. This is done in Section 2.3. The

ring $\mathbf{GBT}_2$ is the subring of $\mathbf{EGBT}_2$ consisting of all the finite sequences (a_k) of $\mathbf{EGBT}_2$; that is, (a_k) is an element of $\mathbf{GBT}_2$ if and only if $a_k \neq 0$ for a finite number of integers k. If I'_k is the ideal of $\mathbf{GBT}_2$ consisting of all sequences whose first k entries are zero, then, as is shown in Section 2.4, the inverse limit of the system $\{\mathbf{GBT}_2/I'_k; k = 1, 2, \dots\}$ is also isomorphic to $\mathbf{Z}_7$.

Remember that $\mathbf{GBT}_2$ is an addressing method. Gibson and Lucas had good geometric reasons to define their carry table for addition in $\mathbf{GBT}_2$ as they did. Consider Figure 5 and recall the standard rules for the addition of two planar vectors. If the hexagon with address 0 is centered at the origin of the plane, then $1 + 2 = 3$, $3 + 6 = 2$ and $5 + 6 = 4$ are all "vectors" inside this first level aggregate. But $3 + 2$, for example, should equal 25 because of the way vectors add. As can be quickly checked, Table 2 shows that $3 + 2$ has a remainder of 5 and a carry of 2, as desired. Consider Figure 6, a third level aggregate, and add 416 to 346. One adds 6 to 6 to get 65, then carries the 6 to the next column and adds to get $1 + 4 + 6 = 4$, then carries the 0 to the next column to get $3 + 4 + 0 = 0$. Thus, $416 + 346 = 45$, which is "vectorially" correct.

The rules of multiplication in $\mathbf{GBT}_2$ are best explained with an example. Multiply 255 by 25.

255 × 25:

$$\begin{array}{rl} 255 & \\ \times\ 25 & \\ \hline 344 & (= 5\times 255) \\ 433 & (= 2\times 255) \\ \hline 604 & (= \text{the GBT sum}) \end{array}$$

Note that there is no carrying during the two modulo 7 multiplications; the only carrying is done in the addition. Figure 6 illustrates this product. Consider Figure 4, and let the origin of the complex plane C be at the center of the hexagon

with address 0. Let the positive real axis pass through the center of the hexagon with address 1, and let the positive imaginary axis pass over the boundary common to the hexagons with addresses 4 and 5. Let C be coordinatized so that the centers of hexagons with addresses 1,5,4,6,2,3 are at the 6^{th} roots of unity $1, e^{2\pi i/6}$, $e^{4\pi i/6}$, $e^{6\pi i/6}$, $e^{8\pi i/6}$, $e^{10\pi i/6}$, respectively. Then the remainder table for multiplication given in Table 2 is just complex multiplication of these roots of unity. There are no carries since a product of two complex numbers each of modulus one is itself a complex number of modulus one.

§2.2. Inverse Limits and p-adic Integers

In this section, a number of definitions and propositions stating the elementary facts concerning inverse limits are presented. These facts will be needed in our proof that $\mathbb{Z}_7$ is isomorphic to $\mathbf{EGBT}_2$.

DEFINITION 2.2.1. *If $A_i (i \in I)$ is a system of groups, indexed by a directed set I, and for each pair $i, j \in I$ with $i \leqslant j$ there is given a homomorphism $\phi_i^j : A_j \to A_i (i \leqslant j)$ such that*

(1) ϕ_i^i is the identity map of A_i, for each $i \in I$, and

(2) for all $i \leqslant j \leqslant k$, we have $\phi_i^j \circ \phi_j^k = \phi_i^k$,

then the system $\mathsf{A} = \{A_i (i \in I); \phi_i^j\}$ is called an inverse system. The inverse limit of this system, $A^* = \varprojlim (A_i; \psi_i^j)$, is defined to consist of all vectors $a = (..., a_i, ...)$ in the direct product $A = \prod_{i \in I} A_i$ for which $\phi_i^j a_j = a_i (i \leqslant j)$ holds.

It is a routine exercise to show that A^* is a subgroup of A. A similar definition can be given for the inverse limit of rings, where it will be the case that A^* is a subring of A.

If $\mathbf{Z}_p^*$ is defined to be the inverse limit of the inverse system $\{\mathbf{Z}/(p^k)(k \in I); \psi_k^l\}$, where $\psi_k^l a_l = a_k$ is defined as $a_k \equiv a_l \bmod(p^k), a_l \in \mathbf{Z}/(p^l), a_k \in \mathbf{Z}/(p^k)$, then the ring $\mathbf{Z}_p^*$ is isomorphic to $\mathbf{Z}_p$. In particular, $\mathbf{Z}_7^*$ is isomorphic to $\mathbf{Z}_7$. The next Proposition makes this last statement more precise.

PROPOSITION 2.2.2. *If* $\mathbf{Z}_p^* = \varprojlim \mathbf{Z}/(p^k)$, *then for each* $\mathbf{a} = (a_1, a_2, ..., a_n, ...) \in \mathbf{Z}_p^*$ *we can associate* $\mathbf{a}$ *with a uniquely determined p-adic integer* $s_1 + s_2 p + ... + s_n p^{n-1} + ...$, *where for all positive integers* n, $0 \leqslant s_n < p$ *and* $a_1 = s_1, a_2 = s_1 + s_2 p, ...,$ $a_n = s_1 + s_2 p + ... + s_n p^{n-1}, ...$.

PROOF: Let (p^k) be the principal ideal of multiples of p^k for $k = 1, 2...$ and any p in $\mathbf{Z}$. Consider the sequence of the rings $\mathbf{Z}/(p), \mathbf{Z}/(p^2), ..., \mathbf{Z}/(p^n), ...$ Define the map ψ_k^l: $\mathbf{Z}/(p^l) \to \mathbf{Z}/(p^k)$ by the congruence relation: $\psi_k^l a_l = a_k$ means $a_k \equiv a_l \bmod p^k$. We have ψ_i^i is the identity map and $\psi_i^j \psi_j^k = \psi_i^k$ if $i \leq j \leq k$. Therefore, we have the inverse system $\{\mathbf{Z}/(p^k)(k \in I); \psi_k^l\}$ and we call its inverse limit the ring of p-adic integers. An element of $\mathbf{Z}_p$ is a sequence of residue classes (or cosets) $(a_1 + (p), a_2 + (p^2), a_3 + (p^3), ...)$ where the a_i's are integers and for $l \geq k$, $a_k \equiv a_l \bmod p^k$. We can represent this element by the sequence of integers $(a_1, a_2, ...)$, where $a_k \equiv a_l \bmod p^k$ for $k \leq l$. Two such sequences $(a_1, a_2, ...)$ and $(b_1, b_2, ...)$ represent the same element if and only if $a_k \equiv b_k \bmod p^k, k = 1, 2, ...$ Addition and multiplication of such sequences is component-wise. If $a \in \mathbf{Z}$, we can write $a = s_1 + s_2 p + ... + s_n p^{n-1}$ where $0 \leq s_i < p$. We can replace the representative $(a_1, a_2, ...)$ in which $a_k \equiv a_l \bmod p^k$ if $k \leq l$ by a representative of the form $(s_1, s_1 + s_2 p, s_1 + s_2 p + s_3 p^2, ...)$ where $0 \leq s_i < p$. In this way we can associate with any element of $\mathbf{Z}_p$ a uniquely determined p-adic number $s_1 + s_2 p + s_3 p^2 + ...$, where $0 \leq s_i < p$. Addition and multiplication of these series corresponding to these

compositions in $\mathbf{Z}_p$ are obtained by applying these compositions on the s_i and "carrying". [10] □

PROPOSITION 2.2.3. *If $C_n =< c_n >$ is the cyclic group of order p^n generated by c_n, and $\phi_n^{n+1} : C_{n+1} \to C_n$ acts as $\phi_n^{n+1} c_{n+1} = c_n$, then $\{C_n(n = 1, 2, ...); \phi_n^m\}$ is an inverse system such that $C^* = \varprojlim C_n$ is isomorphic to $\mathbf{Z}_p$ as an Abelian group.*

PROOF: If ϕ_n denotes the canonical map $C^* \mapsto C_n$, and if we define $\sigma_n : \mathbf{Z}_p \mapsto C_n$ by $\sigma_n(1) = c_n$ $(1 \in \mathbf{Z}_p)$, then there is a unique $\sigma : \mathbf{Z}_p \mapsto C^*$ such that $\phi_n \sigma = \sigma_n$. Since no none zero element of $\mathbf{Z}_p$ belongs to every $\mathbf{Ker}\sigma_n$, $\mathbf{Ker}\sigma = 0$. If $c = (c_1', \ldots, c_n', \ldots) \in C^*$ with $c_n' = k_n c_n$ $(k_n \in \mathbf{Z})$, then by the choice of ϕ_n^{n+1} we have $k_{n+1} \equiv k_n \mod p^n$, and there is a p-adic integer τ such that $\tau \equiv k_n \mod p^n$ for every n. Thus $\sigma(\tau) = c_n'$, and σ must be epic [4]. □

COROLLARY 2.2.4. *If C_n is a ring with multiplicative identity 1_n, which has the property that C_n is generated(under addition) by 1_n and has order p^n (n=1,2,...), and $\phi_n^{n+1} : C_{n+1} \to C_n$ is defined by $\phi_n^{n+1} 1_{n+1} = 1_n$ (i.e. generator goes to generator), then ϕ_n^{n+1} is a ring homomorphism and $\{C_n(n = 1, 2, ...); \phi_n^m\}$ is an inverse system of rings such that $C^* = \varprojlim C_n$ is isomorphic to $\mathbf{Z}_p$.*

The Corollary 2.2.4 follows immediately from Proposition 2.2.3 since the multiplicative structure is essentially additive.

We can also think of $\mathbf{Z}_p$ as the completion of $\mathbf{Z}$ with respect to the absolute value $|\ |_p$ [2,13,26]. Here,

$$|n|_p = p^{-ord_p(n)}$$

where $ord_p(n)$ is the highest exponent to which p divides n. The idea is that two integers are close if their difference is 0 modulo a high power of p. The completion contains the subring of $\mathbf{Q}$ known as the *p-integral* numbers (rational numbers whose denominators are not divisible by p).

If m is a positive integer, m has a finite base p expansion

$$m = m_1 + m_2 p + m_3 p^2 + m_4 p^3 + ... + m_r p^{r-1},$$

where the m_i's are integers between 0 and $p-1$. This expansion (the p-adic expansion for m) will be denoted by its digits, and we will write

$$m = m_1 m_2 m_3 ... m_r.$$

It's easy to see that $ord_p(n)$ is the smallest integer k such that $m_k > 0$. It follows that two integers are close if their p-adic expansions agree for many places. In particular, the sequence

$$1, 11, 111, 1111, 11111, ...$$

is Cauchy, and its limit in $\mathbf{Z}_p$ can be calculated from the usual formula for the limit of a convergent geometric series

$$1111111\cdots = 1 + p + p^2 + p^3 + p^4 + \cdots = \frac{1}{p-1}.$$

(Notice that the common ratio in this series is p, and $|p|_p = \frac{1}{p}$.) Since every p-adic integer is the limit of some Cauchy sequence of integers, and since the p-adic expansions for these integers agree for arbitrarily long initial strings, we can think of a p-adic integer as an infinite p-adic expansion, denoted by an infinite string of digits

$$s_1 s_2 s_3 s_4 s_5 \cdots = s_1 + s_2 p + s_3 p^2 + s_4 p^3 + s_5 p^4 + \ldots.$$

where each s_i is an integer between 0 and $p-1$. As with all completions, $|\ |_p$ extends to a valuation on $\mathbf{Z}_p$, and its value can be calculated by the same formula

that defines it on $\mathbb{Z}$ ($ord_p(a)$ is the smallest integer k such that $a_k > 0$). So, just as in $\mathbb{Z}$, two p-adic integers are close if their representations agree for many digits (that is, if their difference is 0 modulo a high power of p). An element of $\mathbb{Z}_p$ is a non-negative integer if and only if its digits are eventually 0; an element of $\mathbb{Z}_p$ is in $\mathbb{Q}$ precisely when its digits eventually repeat.

Given a p-adic integer a, a fundamental system of neighborhoods for a is the sequence

$$\{a + p^n\mathbb{Z}_p : n = 0, 1, 2, 3, ...\}.$$

Indeed, given an integer n, $\mathbb{Z}_p$ splits up into p^n disjoint disks of diameter $\frac{1}{p^n}$, namely the cosets in $\mathbb{Z}_p/p^n\mathbb{Z}_p$. Two p-adic integers x and y are within $\frac{1}{p^n}$ of each other if and only if they belong to the same disk.

The metric d defined by $|\ |_p$ satisfies a stronger condition than the triangle inequality; if a, b and c are in $\mathbb{Z}_p$, then

$$d(a, b) \leq max\{d(a, c), d(b, c)\}$$

(equality holds if $d(a, c)$ and $d(b, c)$ are unequal). This non-archimedean property of d implies that every triangle is isosceles and that every point interior to a circle is its center.

§2.3. The 2-Dimensional Extended Generalized Balanced Ternary Numbers

PROPOSITION 2.3.1. *The subring* $I_k = \{(\underbrace{0, ..., 0}_{k}, x_{k+1}, x_{k+2}, ...) : x_i \in \mathbb{Z}/(7)$ *for all* $i \geq k + 1\}$ *is an ideal in* $\mathbf{EGBT_2}$ *for all* $k = 1, 2, \ldots$.

PROOF: If y $= (y_1, y_2, ..., y_n, ...) \in \mathbf{EGBT_2}$ and x $= (\underbrace{0, ...0}_{k}, x_{k+1}, x_{k+2}, ...) \in I_k$, then by the rules of multiplication and the carries rules given in Table 2 xy =

$(\underbrace{0,...,0}_{k}, x_{k+1}y_1, x_{k+2}y_1 + x_{k+1}y_2 + c_{k+2}, ...)$. Therefore, xy $\in I_k$, yx $\in I_k$ and I_k is an ideal in $\mathbf{EGBT}_2$. □

PROPOSITION 2.3.2. *For each positive integer k the cardinality of* $\mathbf{EGBT}_2/I_k$ *is* 7^k.

PROOF: The set $\mathbf{EGBT}_2/I_k = \{(a_1, a_2, ..., a_k, 0, ...) + I_k : a_i \in \mathbb{Z}/(7)$ for all $i = 1, 2, ...\}$. Since there are 7 choices for each a_i in each of the first k components, there are 7^k choices for $(a_1, a_2, ..., a_k, 0, ...) + I_k$. Therefore, the cardinality of $\mathbf{EGBT}_2/I_k$ is 7^k. □

Note: In the following lemmas and propositions an arbitrary value will be denoted by the symbol *. It may be the case that * will represent one value on one side of an equation or expression and another on the other side.

LEMMA 2.3.3. *In the ring* $\mathbf{EGBT}_2$, *the following relations hold.*

$$1.\ \underbrace{(1,*) + ... + (1,*)}_{l} = \begin{cases} (0,5,*), & \text{if } l = 7 \\ (x_1,*), & \text{if } l < 7, \text{ where } x_1 \text{ is a nonzero element in } \mathbb{Z}/(7) \end{cases};$$

$$2.\ \underbrace{(2,*) + ... + (2,*)}_{l} = \begin{cases} (0,3,*), & \text{if } l = 7 \\ (x_1,*), & \text{if } l < 7, \text{ where } x_1 \text{ is a nonzero element in } \mathbb{Z}/(7) \end{cases};$$

$$3.\ \underbrace{(3,*) + ... + (3,*)}_{l} = \begin{cases} (0,1,*), & \text{if } l = 7 \\ (x_1,*), & \text{if } l < 7, \text{ where } x_1 \text{ is a nonzero element in } \mathbb{Z}/(7) \end{cases};$$

$$4.\ \underbrace{(4,*) + ... + (4,*)}_{l} = \begin{cases} (0,6,*), & \text{if } l = 7 \\ (x_1,*), & \text{if } l < 7, \text{ where } x_1 \text{ is a nonzero element in } \mathbb{Z}/(7) \end{cases};$$

$$5.\ \underbrace{(5,*)+\ldots+(5,*)}_{l} = \begin{cases} (0,4,*), & \text{if } l = 7 \\ (x_1,*), & \text{if } l < 7, \text{ where } x_1 \text{ is a nonzero element in } \mathbb{Z}/(7) \end{cases};$$

$$6.\ \underbrace{(6,*)+\ldots+(6,*)}_{l} = \begin{cases} (0,2,*), & \text{if } l = 7 \\ (x_1,*), & \text{if } l < 7, \text{ where } x_1 \text{ is a nonzero element in } \mathbb{Z}/(7) \end{cases}.$$

PROOF: It is a routine (but lengthy) computation to verify these identities. We found a simple Fortran program to be a convenient tool to check that these calculations are correct. □

LEMMA 2.3.4. *In the ring* $\mathbf{EGBT}_2$, *if* $l = 7^n$, *then*

$$\underbrace{(1,*)+\ldots+(1,*)}_{l} = \begin{cases} (\underbrace{0,\ldots,0}_{n},5,*), & \text{if } n = 1 \ mod(6) \\ (\underbrace{0,\ldots,0}_{n},4,*), & \text{if } n = 2 \ mod(6) \\ (\underbrace{0,\ldots,0}_{n},6,*), & \text{if } n = 3 \ mod(6) \\ (\underbrace{0,\ldots,0}_{n},2,*), & \text{if } n = 4 \ mod(6) \\ (\underbrace{0,\ldots,0}_{n},3,*), & \text{if } n = 5 \ mod(6) \\ (\underbrace{0,\ldots,0}_{n},1,*), & \text{if } n = 0 \ mod(6) \end{cases}.$$

PROOF:

Case 1. If $n = 1$ and $l = 7$, then by Lemma 2.3.3.1

$$\underbrace{(1,*)+\ldots+(1,*)}_{7} = (0,5,*)$$

Case 2. If $n = 2$ and $l = 7^2$, then by Case 1 and Lemma 2.3.3.5

$$\underbrace{(1,*) + \ldots + (1,*)}_{7^2} = \underbrace{(1,*) + \ldots + (1,*)}_{7} + \underbrace{(1,*) + \ldots + (1,*)}_{7} + \ldots + \underbrace{(1,*) + \ldots + (1,*)}_{7}$$

$$= \underbrace{(0,5,*) + (0,5,*) + \ldots + (0,5,*)}_{7} = (0,0,4,*)$$

Case 3. If $n = 3$ and $l = 7^3$, then by Case 2 and Lemma 2.3.3.4

$$\underbrace{(1,*) + \ldots + (1,*)}_{7^3} = \underbrace{(1,*) + \ldots (1,*)}_{7^2} + \underbrace{(1,*) + \ldots + (1,*)}_{7^2} + \ldots + \underbrace{(1,*) + \ldots + (1,*)}_{7^2}$$

$$= \underbrace{(0,0,4,*) + (0,0,4,*) + \ldots + (0,0,4,*)}_{7} = (0,0,0,6,*)$$

Case 4. If $n = 4$ and $l = 7^4$, then by Case 3 and Lemma 2.3.3.6

$$\underbrace{(1,*) + \ldots + (1,*)}_{7^4} = \underbrace{(1,*) + \ldots (1,*)}_{7^3} + \underbrace{(1,*) + \ldots + (1,*)}_{7^3} + \ldots + \underbrace{(1,*) + \ldots + (1,*)}_{7^3}$$

$$= \underbrace{(0,0,0,6,*) + (0,0,0,6,*) + \ldots + (0,0,0,6,*)}_{7} = (0,0,0,0,2,*)$$

Case 5. If $n = 5$ and $l = 7^5$, then by Case 4 and Lemma 2.3.3.2

$$\underbrace{(1,*)+...+(1,*)}_{7^5} = \underbrace{(1,*)+...(1,*)}_{7^4}+\underbrace{(1,*)+...+(1,*)}_{7^4}+...+\underbrace{(1,*)+...+(1,*)}_{7^4}$$

$$= \underbrace{(0,0,0,0,2,*)+(0,0,0,0,2,*)+...+(0,0,0,0,2,*)}_{7} = (0,0,0,0,0,3,*)$$

Case 6. If $n = 6$ and $l = 7^6$, then by Case 5 and Lemma 2.3.3.3

$$\underbrace{(1,*)+...+(1,*)}_{7^6} = \underbrace{(1,*)+...(1,*)}_{(1)7^5}+\underbrace{(1,*)+...+(1,*)}_{(2)7^5}+...+\underbrace{(1,*)+...+(1,*)}_{(7)7^5}$$

$$= \underbrace{(0,0,0,0,0,3,*)}_{(1)}+\underbrace{(0,0,0,0,0,3,*)}_{(2)}+...+\underbrace{(0,0,0,0,0,3,*)}_{(7)}$$

$$= (0,0,0,0,0,0,1,*)$$

By inductively repeating the six steps in the process indicated above, we have the conclusion of the Lemma. □

COROLLARY 2.3.5. *If $l = 7^n$ for some integer n, then $\underbrace{(1,*)+...+(1,*)}_{l} = (\underbrace{0,...0}_{n}, x_{n+1}, *)$, where x_{n+1} is some nonzero element in* $\mathbf{Z}/(7)$.

PROOF: From the six patterns in Lemma 2.3.4, we know that if $l = 7^n$, then $\underbrace{(1,*)+...+(1,*)}_{7^n} = (\underbrace{0,...,0}_{n}, x_{n+1}, *)$, where x_{n+1} is different from zero. □

LEMMA 2.3.6. *In the ring* $\mathbf{EGBT}_2$, *if $l = 7^n$, then $\underbrace{(1,*)+...+(1,*)}_{l} = (\underbrace{0,...,0}_{n}, x_{n+1}, *)$, where x_{n+1} is different from zero, and if $l < 7^n$, then $\underbrace{(1,*)+...+(1,*)}_{l} = (x_1, ..., x_n, *)$, where x_i is different from zero for some integer i between 1 and n.*

PROOF: The proof will be by induction on the integer n.

If $n = 1$, then by Lemma 2.3.3.1 $\underbrace{(1,*) + ... + (1,*)}_{l} = (0,5,*)$ for $l = 7$ and $\underbrace{(1,*) + ... + (1,*)}_{l} = (x_1,*)$ for $l < 7$, where x_1 is different from zero. Therefore, the inductive step is true for $n = 1$.

Assume that the inductive step is true for all integers less than or equal n (i.e. $l \leq 7^n$).

If $l = 7^{n+1}$, then by Corollary 2.3.5

$$\underbrace{(1,*) + ... + (1,*)}_{l} = (\underbrace{0,...,0}_{n+1}, x_{n+2}, *), \text{ where } x_{n+2} \text{ is different from zero.}$$

If $l < 7^{n+1}$ (i.e. $l = h7^n + l'$ where $h < 7$ and $l' < 7^n$), then by Corollary 2.3.5 we have

$$\underbrace{(1,*) + ...(1,*)}_{l} = \underbrace{(1,*) + ... + (1,*)}_{h7^n} + \underbrace{(1,*) + ... + (1,*)}_{l'}$$

$$= \underbrace{(1,*) + ... + (1,*)}_{7^n} + ... + \underbrace{(1,*) + ... + (1,*)}_{7^n} + \underbrace{(1,*) + ... + (1,*)}_{l'}$$

$$= (\underbrace{0,...,0}_{n}, (hx_{n+1}) \mod 7, *) + \underbrace{(1,*) + ... + (1,*)}_{l'}.$$

By the induction assumption we have $\underbrace{(1,*) + ... + (1,*)}_{l'} = (x_1, x_2, ...x_n, *)$, where some x_i is different from zero if and only if l' is different from zero.

Thus, if $l' \neq 0$, then by induction $x_i \neq 0$ for some $i \leq n$. If $l' = 0$, then by induction $x_{n+1} \neq 0$. Since $h \neq 0$, $(hx_{n+1}) \mod 7 \neq 0$. Therefore, the induction is true for the integer $n+1$. □

PROPOSITION 2.3.7. *The ring* $\mathbf{EGBT}_2/I_k$ *is generated (under addition) by the element* $\bar{1}_k = (1,0,0,...) + I_k \in \mathbf{EGBT}_2/I_k$.

PROOF: By Lemma 2.3.6, we have:

$$\underbrace{\bar{1}_k + ... + \bar{1}_k}_{l} = \underbrace{(1,0,0,...) + I_k + ... + (1,0,0,...) + I_k}_{l}$$

$$= \underbrace{(1,0,0,...) + ... + (1,0,0,...)}_{l} + I_k$$

$$= \begin{cases} (\underbrace{0,...,0}_{k}, x_{k+1}, *) + I_k, & \text{if } l = 7^k \\ (x_1, ..., x_k, *) + I_k, & \text{if } l < 7^k, \text{ where } x_i \neq 0 \text{ for some } i \in \{1, ...k\} \end{cases}.$$

Thus, $\underbrace{\bar{1}_k + ... + \bar{1}_k}_{l} = I_k$ if and only if $l = 7^k$. Therefore, the order of $\bar{1}_k$ is 7^k. By Proposition 2.3.2, $\bar{1}_k$ is a generator of the ring $\mathbf{EGBT}_2/I_k$ under addition. □

PROPOSITION 2.3.8. *If* $\phi_k^l : \mathbf{EGBT}_2/I_l \to \mathbf{EGBT}_2/I_k$ *is defined by* $\phi_k^l \bar{1}_l = \bar{1}_k$, *then* $\{\mathbf{EGBT}_2/I_k (k = 1,2,...); \phi_k^l\}$ *is an inverse system. If* $\mathbf{EGBT}_2{}^* = \varprojlim(\mathbf{EGBT}_2/I_k; \phi_k^l)$, *then* $\mathbf{EGBT}_2{}^*$ *is isomorphic to* $\mathbf{Z}_7$ *and* $\mathbf{EGBT}_2{}^* = \{ ((x_1, 0, ...) + I_1, (x_1, x_2, 0, ...) + I_2, ...); x_k \in \mathbf{Z}/(7)$ *for* $k = 1, 2, ... \}$.

PROOF: By Proposition 2.3.2 we know that $\mathbf{EGBT}_2/I_k$ has order 7^k for all positive integers k. By Proposition 2.3.7 we know that $\mathbf{EGBT}_2/I_k$ is generated (under addition) by $\bar{1}_k$ for all positive integers k. Thus, by Corollary 2.2.4, $\{\mathbf{EGBT}_2/I_k (k = 1,2,...); \phi_k^l\}$ is an inverse system, and $\mathbf{EGBT}_2{}^* = \varprojlim(\mathbf{EGBT}_2/I_k; \phi_k^l)$ is isomorphic to $\mathbf{Z}_7$.

Let S denote the set $\{ ((x_1, 0, ...) + I_1, (x_1, x_2, 0, ...) + I_2, ...); x_k \in \mathbf{Z}/(7)$ for $k = 1, 2, ... \}$. It is easy to see that $S \subseteq \mathbf{EGBT}_2{}^*$. Let $\bar{x} = (\bar{x}_1, \bar{x}_2, ..., \bar{x}_k, ...) \in \mathbf{EGBT}_2{}^*$, where $\bar{x}_k = (x_1, x_2, ...x_k, 0, ...) + I_k \in \mathbf{Z}/(I_k)$ (k=1,2,...). By Proposition 3.7, $\bar{x}_k = m\bar{1}_k$ where $m \in \mathbf{Z}/(7^k)$. Therefore, $\phi_k^l \bar{x}_l = m\bar{1}_k = m((1,0,...) + I_k) = (x_1, x_2, ..., x_k, *) + I_k = (x_1, x_2, ..., x_k, 0, ...) + I_k$. This last equation shows that $\bar{x}_k = (x_1, x_2, ..., x_k, 0, ...) + I_k$, and $\bar{x} = ((x_1, 0, ...) + I_1, (x_1, x_2, 0, ...) + I_2, ... , (x_1, x_2, ..., x_k, 0, ...) + I_k, ...)$. Therefore, $\mathbf{EGBT}_2{}^* \subseteq S$ and $\mathbf{EGBT}_2{}^* = S$. □

PROPOSITION 2.3.9. *The ring* $\mathbf{EGBT_2}$ *is isomorphic to* $\mathbf{EGBT_2}^*$.

PROOF:

Define the function η: $\mathbf{EGBT_2} \to \mathbf{EGBT_2}^*$ by $\eta(x_1, x_2, ...) = ((x_1, 0, ...) + I_1, (x_1, x_2, 0, ...) + I_2, ...)$ for all $(x_1, x_2, ...) \in \mathbf{EGBT_2}$.

We will now show that η is an isomorphism.

(1) It is straightforward to show that η is well defined and surjective.

(2) The function η is injective.

Let $x = (x_1, x_2, ...)$ and $y = (y_1, y_2, ...)$ be elements in $\mathbf{EGBT_2}$. If $\eta(x) = \eta(y)$, then $(\ (x_1, 0, ...) + I_1, (x_1, x_2, 0, ...) + I_2, ...\ ) = (\ (y_1, 0, ...) + I_1, (y_1, y_2, 0, ...) + I_2, ...)$. This equation implies that $(x_1, 0, ...) + I_1 = (y_1, 0, ...) + I_1$, $(x_1, x_2, 0, ...) + I_2 = (y_1, y_2, ...) + I_2$, ... $(x_1, x_2, ...x_n, 0, ...) + I_n = (y_1, y_2, ...y_n, 0, ...) + I_n$, ..., which implies that $(x_1 - y_1, 0, ...) \in I_1$, $(x_1 - y_1, x_2 - y_2, 0, ...) \in I_2$, ..., $(x_1 - y_1, x_2 - y_2, ..., x_n - y_n, 0, ...) \in I_n$, ... for all integers n. Thus, we have $x_1 = y_1$, $x_2 = y_2$, ..., $x_n = y_n$, ... for all integers n. Therefore, $x = y$ and η is injective.

(3) The function η is a ring homomorphism.

If $x = (x_1, x_2, ...)$ and $y = (y_1, y_2, ...)$ are elements in $\mathbf{EGBT_2}$, then $x + y = (s_1, s_2, ..., s_n, ...)$, where $x_1 + y_1 = c_2 7 + s_1$, ..., $x_n + y_n + c_n = c_{n+1} 7 + s_n$, ... for all integers n, and $xy = (t_1, t_2, ...t_n, ...)$, where $x_1 y_1 = c_2 7 + t_1$, ..., $x_1 y_n + x_2 y_{n-1} + ... + x_n y_1 + c_n = c_{n+1} 7 + t_n$ for all integers n. Thus, $\eta(x + y) = (\ (s_1, 0, ...) + I_1$, ..., $(s_1, s_2, ..., s_n, ...) + I_n$, ...), and $\eta(xy) = (\ (t_1, 0, ...) + I_1$, ..., $(t_1, t_2, ..., t_n, 0, ...) + I_n$, ...). Since $\eta(x) + \eta(y) = (\ (x_1, 0, ...) + I_1$, ..., $(x_1, x_2, ...x_n, 0, ...) + I_n$, ...) + $(\ (y_1, 0, ...) + I_1$, ..., $(y_1, y_2, ...y_n, 0, ...) + I_n$, ...) = $(\ (x_1, 0, ...) + (y_1, 0, ...) + I_1$, ..., $(x_1, x_2, ..., x_n, 0, ...) + (y_1, y_2, ..., y_n, 0, ...) + I_n$, ...) = $(\ (s_1, 0, ...) + I_1$, ..., $(s_1, s_2, ...s_n, 0, ...) + I_n$, ...), we have $\eta(x) + \eta(y) = \eta(x + y)$. Since $\eta(x)\eta(y) = (\ (x_1, 0, ...) + I_1$, ..., $(x_1, ...x_n, 0, ...) + I_n$, ... $)(\ (y_1, 0, ...) + I_1$, ..., $(y_1, ..., y_n, 0, ...) + I_n$, ...) = $(\ (x_1, 0, ..)(y_1, 0, ...) + I_1$, ..., $(x_1, ..., x_n, 0, ...)\ (y_1, ..., y_n, 0, ...) + I_n$, ...) =

$((t_1, 0, ...) + I_1, ..., (t_1, ..., t_n, 0, ...) + I_n, \ ...)$, we have $\eta(x)\eta(y) = \eta(xy)$. Therefore, η is a ring homomorphism.

Thus by (1),(2) and (3), the map η is a ring isomorphism from $\mathbf{EGBT}_2$ to $\mathbf{EGBT}_2{}^*$. □

THEOREM 2.3.10. $\mathbf{EGBT}_2$ *is isomorphic to* $\mathbf{Z}_7$.

PROOF: By Proposition 2.3.9, $\mathbf{EGBT}_2 \cong \mathbf{EGBT}_2{}^*$. By Proposition 2.3.8, $\mathbf{EGBT}_2{}^* \cong \mathbf{Z}_7$. Therefore, $\mathbf{EGBT}_2 \cong \mathbf{Z}_7$. □

§2.4. The 2-dimensional Generalized Balanced Ternary Numbers

The 2-dimensional Generalized Balanced Ternary Numbers, denoted by $\mathbf{GBT}_2$, are the subring of $\mathbf{EGBT}_2$ consisting of all the finite sequences of $\mathbf{EGBT}_2$. For convenience of notion we will use G to denote $\mathbf{GBT}_2$.

Lucas proved that G/I'_k is isomorphic to $\mathbf{Z}/(7^k)$, where I'_k is the ideal of G consisting of all those sequences whose first k digits are zero. We will now show that the inverse limit of G/I'_k is isomorphic to $\mathbf{EGBT}_2$.

PROPOSITION 2.4.1. *For each positive integer* k *the cardinality of* G/I'_k *is* 7^k.

PROOF: The proof is the same as the proof of Proposition 2.3.2. □

PROPOSITION 2.4.2. *The ring* G/I'_k *is generated (under addition) by the element* $\bar{1}_k$ = *(1,0,0,...)* + $I'_k \in G/I'_k$.

PROOF: Since the results of Lemmas 2.3.3, 2.3.4, 2.3.5 and 2.3.6 are true in the subring G, we can follow the same proof given for Proposition 2.3.7. □

THEOREM 2.4.3. *If* ψ^l_k: $G/I'_l \to G/I'_k$ *is defined by* $\psi^l_k \bar{1}_l = \bar{1}_k$, *then* $\{G/I'_k (k = 1, 2, ...); \psi^l_k\}$ *is an inverse system. If* $G^* = \varprojlim (G/I'_k; \psi^l_k)$, *then* G^* *is isomorphic to both* $\mathbf{Z}_7$ *and* $\mathbf{EGBT}_2$.

PROOF: By Proposition 2.4.1, G/I_k' has order 7^k for any positive integer k. By Proposition 2.4.2, G/I_k' is generated by $\bar{1}_k$ for any positive integer k. Thus, by Corollary 2.2.4, $\{G/I_k'(k=1,2,...);\psi_k^l\}$ is an inverse system, and $G^* = \varprojlim(G/I_k', \psi_k^l)$ is isomorphic to $\mathbf{Z}_7$. By Theorem 2.3.10, $\mathbf{Z}_7$ is isomorphic to $\mathbf{EGBT}_2$. Therefore, G^* is isomorphic to $\mathbf{EGBT}_2$. □

§2.5. 15-adic Integers and the Ring $\mathbf{EGBT}_3$

Guided by algebraic rules motivated by a truncated octahedral tiling in 3-dimensional space, L. Gibson and D. Lucas [6] defined rules for addition and multiplication for the 3-dimensional Generalized Balanced Ternary Numbers. (For a diagram of the truncated octahedron see Figure (4,6,6) in Toth [27].) The carry rules have been modified to those presented in Table 3 while the remainder rules remain the same as the rules known for the ring of 15-adic integers. The extended 3-dimensional Generalized Balanced Ternary Numbers are the set of all sequences $\{(a_1, a_2, a_3, ...) : 0 \leq a_k < 15\}$ with the same addition and multiplication as defined for the 3-dimensional Generalized Balanced Ternary Numbers. It can be shown that the resulting structure forms a commutative ring with unity. We use $\mathbf{EGBT}_3$ to denote this ring. The following lemmas and proposition can be proved in a way similar to the proofs in section 2.3. Therefore, we conclude that $\mathbf{EGBT}_3$ is isomorphic to the ring of 15-adic integers.

LEMMA 2.5.1. *In the ring* $\mathbf{EGBT}_3$, *the following relations hold.*

$$1.\ \underbrace{(1,*)+...+(1,*)}_{l} = \begin{cases} (0,2,*), & \text{if } l = 15 \\ (x_1,*), & \text{if } l < 15, \text{ where } x_1 \text{ is a nonzero element in } \mathbf{Z}/(15) \end{cases};$$

$$2.\ \underbrace{(2,*)+\ldots+(2,*)}_{l}=\begin{cases}(0,4,*), & \text{if } l=15\\ (x_1,*), & \text{if } l<15, \text{ where } x_1 \text{ is a nonzero element in } \mathbf{Z}/(15)\end{cases};$$

$$3.\ \underbrace{(4,*)+\ldots+(4,*)}_{l}=\begin{cases}(0,8,*), & \text{if } l=15\\ (x_1,*), & \text{if } l<15, \text{ where } x_1 \text{ is a nonzero element in } \mathbf{Z}/(15)\end{cases};$$

$$4.\ \underbrace{(8,*)+\ldots+(8,*)}_{l}=\begin{cases}(0,1,*), & \text{if } l=15\\ (x_1,*), & \text{if } l<15, \text{ where } x_1 \text{ is a nonzero element in } \mathbf{Z}/(15)\end{cases}.$$

LEMMA 2.5.2. *In the ring* $\mathbf{EGBT}_3$, *if* $l=15^n$, *then*

$$\underbrace{(1,*)+\ldots+(1,*)}_{l}=\begin{cases}(\underbrace{0,\ldots,0}_{n},2,*), & \text{if } n=1 \mod(4)\\ (\underbrace{0,\ldots,0}_{n},4,*), & \text{if } n=2 \mod(4)\\ (\underbrace{0,\ldots,0}_{n},8,*), & \text{if } n=3 \mod(4)\\ (\underbrace{0,\ldots,0}_{n},1,*), & \text{if } n=0 \mod(4)\end{cases}.$$

COROLLARY 2.5.3. *If* $l=15^n$ *for some integer* n, *then* $\underbrace{(1,*)+\ldots+(1,*)}_{l}=(\underbrace{0,\ldots 0}_{n},x_{n+1},*)$, *where* x_{n+1} *is some nonzero element in* $\mathbf{Z}/(15)$.

LEMMA 2.5.4. *In the ring* $\mathbf{EGBT}_3$, *if* $l=15^n$, *then* $\underbrace{(1,*)+\ldots+(1,*)}_{l}=(\underbrace{0,\ldots,0}_{n},x_{n+1},*)$, *where* x_{n+1} *is different from zero, and if* $l<15^n$, *then* $\underbrace{(1,*)+\ldots+(1,*)}_{l}=(x_1,\ldots,x_n,*)$, *where* x_i *is different from zero for some integer* i *between 1 and* n.

PROPOSITION 2.5.5. *The ring* $\mathbf{EGBT}_3/I_k$ *is generated (under addition) by the element* $\bar{1}_k=(1,0,0,\ldots)+I_k\in\mathbf{EGBT}_3/I_k$.

Table 1. Digitwise Operations on $\mathbb{Z}_7$

Remainder

+	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

Carry

+	1	2	3	4	5	6
1	0	0	0	0	0	1
2	0	0	0	0	1	1
3	0	0	0	1	1	1
4	0	0	1	1	1	1
5	0	1	1	1	1	1
6	1	1	1	1	1	1

Remainder

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Carry

×	1	2	3	4	5	6
1	0	0	0	0	0	0
2	0	0	0	1	1	1
3	0	0	1	1	2	2
4	0	0	1	2	2	3
5	0	1	2	2	3	4
6	0	1	2	3	4	5

Table 2. Digitwise Operations on $\mathbf{EGBT}_2$

Remainder

+	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

Carry

+	1	2	3	4	5	6
1	1	0	3	0	1	0
2	0	2	2	0	0	6
3	3	2	3	0	0	0
4	0	0	0	4	5	4
5	1	0	0	5	5	0
6	0	6	0	4	0	6

Remainder

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Carry

×	1	2	3	4	5	6
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0

Table 3. The carry tables for the 3-dimensional **GBT**.

Carry

+	1	2	3	4	5	6	7	8	9	A	B	C	D	E
1	1	0	3	0	1	0	7	0	1	0	3	0	1	0
2	0	2	2	0	0	6	6	0	0	2	2	0	0	E
3	3	2	3	0	7	6	7	0	3	2	3	0	0	0
4	0	0	0	4	4	4	4	0	0	0	0	C	D	C
5	1	0	7	4	5	4	7	0	1	0	0	D	D	0
6	0	6	6	4	4	6	6	0	0	E	0	C	0	E
7	7	6	7	4	7	6	7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	8	9	8	B	8	9	8
9	1	0	3	0	1	0	0	9	9	B	B	9	9	0
A	0	2	2	0	0	E	0	8	B	A	B	8	0	E
B	3	2	3	0	0	0	0	B	B	B	B	0	0	0
C	0	0	0	C	D	C	0	8	9	8	0	C	D	C
D	1	0	0	D	D	0	0	9	9	0	0	D	D	0
E	0	E	0	C	0	E	0	8	0	E	0	C	0	E

Carry

×	1	2	3	4	5	6	7	8	9	A	B	C	D	E
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	6	0	0	C	0	0	3	0	0	9	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	5	0	0	0	0	A	0	0	0	0
6	0	0	C	0	0	9	0	0	6	0	0	3	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	3	0	0	6	0	0	9	0	0	C	0	0
A	0	0	0	0	A	0	0	0	0	5	0	0	0	0
B	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C	0	0	9	0	0	3	0	0	C	0	0	6	0	0
D	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E	0	0	0	0	0	0	0	0	0	0	0	0	0	0

CHAPTER 3

THE p – adic INTEGERS AND THE RING $\mathbf{EGBT_n}$

§3.1. Introduction

Recall that for integer $n \geq 2$ the $\mathbf{GBT}_n$ is the set of all finite sequences $(a_1, a_2, \ldots, a_k), k = 1, 2, \ldots$, with entries from the set of integers $\{0, 1, \ldots, 2^{n+1} - 2\}$. The $\mathbf{EGBT}_n$ is the set of all infinite sequences $(a_1, a_2, \ldots)$ with entries from $\{0, 1, \ldots, 2^{n+1} - 2\}$. Since the integer $2^{n+1} - 1$ may not necessarily be a prime number, from now on we will denote $2^{n+1} - 1$ by q and will refer to the q-adic integers.

Lucas has defined an addition and multiplication upon $\mathbf{GBT}_n$ that makes it into a commutative ring with unity [15]. These definitions will be presented in Section 3.2 once enough notation has been developed to express these definitions in a simple manner. Extending these operations in a natural way makes $\mathbf{EGBT}_n$ also into a commutative ring with unity [15].

As previously stated, the main result of this chapter is that $\mathbf{EGBT}_n$ is isomorphic as a ring to the q-adic integers for certain values of n.

§3.2. The Carry Tables of $\mathbf{EGBT}_n$

DEFINITION 3.2.1. *Let S_n denote the set of all sequences of the form $s_n ... s_0$ such that s_i equals 0 or 1 for all $i = 0, 1, ...n$. The sequence of all ones is identified with*

the sequence of all zeros. Let B_q *be the function from the set* $\mathbb{Z}/(q)$ *to the set* S_n *defined by the rule that if* $x = s_n 2^n + ... + s_1 2 + s_0$, *then* $B_q(x) = s_n...s_0$.

It is clear that B_q is a bijective map and that the inverse of B_q, denoted by B_q^{-1}, is the map from S_n to $\mathbb{Z}/(q)$ defined by $B_q^{-1}(s_n...s_0)=s_n 2^n+...+s_1 2+s_0$.

DEFINITION 3.2.2. *Let* T *be the function from* S_n *to* S_n *defined by* $T(s_n...s_0) = s_{n-1}...s_0 s_n$, *where* $s_n...s_0$ *is any element in* S_n.

The composition of T with itself i times is denoted by T^i. For any $s_n...s_0 \in S_n$, $T^i(s_n...s_0) = s_i...s_0 s_n...s_{i+1}$. The inverse of T is denoted by T^{-1}, and is defined by $T^{-1}(s_n...s_0) = s_0 s_n...s_1$. The function T is a twist(or shift) to the left of the binary sequences and the function T^{-1} is a twist to the right.

DEFINITION 3.2.3. *Let* E *be the function from* $S_n \times S_n$ *to* S_n *defined by* $E(r_n...r_0, s_n...s_0) = t_n...t_0$, *where* $t_i = (r_i + s_i) \mod 2$ *for* $i = 0, 1, ..., n$.

Note that E is the well known *exclusive or* function.

Since the associative law holds for the binary operation E in S_n, it is understood that $E(r_n...r_0, s_n...s_0, t_n...t_0) = E(E(r_n...r_0, s_n...s_0), t_n...t_0)$.

In the n-dimensional algebraic structure **GBT**, the addition of any two digits x and $y \in \mathbb{Z}/(q)$ yields a remainder r defined as the residue of $x + y$ modulo q. Note that this is analogous to the usual rules for base 10 arithmetic. The carry $C(x, y)$ defined by D. Lucas [6,7] is the following.

DEFINITION 3.2.4. *Let* C *denote the function from* $\mathbb{Z}/(q) \times \mathbb{Z}/(q)$ *to the set* $\mathbb{Z}/(q)$ *defined by* $C(x, y) = B_q^{-1}(T^{-1}(E(B_q(x), B_q(y), B_q(r))))$, *where* r *is the remainder of* $x + y \mod q$.

Heuristically, the carry $C(x, y)$ is defined by first converting x, y and r to binary sequences, second, adding using the exclusive or, third twisting the resulting

sequence one unit to the right, and, finally, converting the resulting binary sequence back to an element in $\mathbb{Z}/(q)$.

It is easy to see that the associative law holds for the carry function C. Therefore, it is understood that $C(x,y,z) = C(C(x,y),z)$.

One is now in the position to define the operations of addition and multiplication that make $\mathbf{GBT}_n$ into a ring.

Let $a = (a_1,\ldots,a_k)$ and $b = (b_1,\ldots,b_l)$ be elements of $\mathbf{GBT}_n$ where, without loss of generality, $k \leq l$. Define the "carries" c_j in the following recursive manner: $c_1 = 0$ and $c_j = C(a_{j-1},b_{j-1}) + C((a_{j-1}+b_{j-1}) \mod q, c_{j-1})$, for $j = 2,\ldots,l$. The sum $a+b$ is now defined to be the finite sequence $r = (r_1,\ldots,r_m)$, where $r_1 \equiv (a_1+b_1) \mod q$ and $r_j \equiv (a_j+b_j+c_j) \mod q$ for $j \geq 2$. (Note that the author is assuming that $a_j = 0$ for $j = k+1,\ldots,l$.)

To define the multiplication requires a little more preparation. Let y and z be elements from the set $\{0,1,\ldots,q-1\}$ with $B_q(z) = z_n \ldots z_0$. Then,

$$\begin{aligned} B_q(y)B_q(z) &= 2^n B_q(y)z_n + \cdots + 2B_q(y)z_1 + B_q(y)z_0 = \\ &= z_n(2^n B_q(y)) + \cdots + z_1(2B_q(y)) + z_0(B_q(y)) = \\ &= z_n T^n(B_q(y)) + \cdots + z_1 T^1(B_q(y)) + z_0 B_q(y). \end{aligned}$$

Set $w_0 = B_q^{-1}(B_q(y)) = y$ and $w_i = B_q^{-1}(T^i(B_q(y)))$ for $i = 1,\ldots,n$. With this notation in place, the following definition is made.

DEFINITION 3.2.5. *Let D denote the function from $\mathbb{Z}/(q)\times\mathbb{Z}/(q)$ into $\mathbb{Z}/(q)$ defined by*

$$\begin{aligned} D(y,z) = {} & C(z_n w_n, z_{n-1}w_{n-1}) + C((z_n w_n + z_{n-1}w_{n-1}) \mod q, z_{n-2}w_{n-2}) + \\ & \cdots + C((z_n w_n + \cdots + z_1 w_1) \mod q, z_0 w_0). \end{aligned}$$

As above, let $a = (a_1,\ldots,a_k)$ and $b = (b_1,\ldots,b_l), k \leq l$, be from $\mathbf{GBT}_n$. Define the "carries" d_j in the following recursive manner: $d_1 = 0$ and $d_j =$

$D(a_1, b_{j-1}) + D(a_2, b_{j-2}) + \cdots + D(a_{j-1}, b_1) + C(a_1 b_{j-1}, a_2 b_{j-2}) + C((a_1 b_{j-1} + a_2 b_{j-2}) \mod q, a_3 b_{j-3}) + \cdots + C((a_1 b_{j-1} + \cdots + a_{j-2} b_2) \mod q, a_{j-1} b_1) + C((a_1 b_{j-1} + \cdots + a_{j-1} b_1) \mod q, d_{j-1})$, for $j = 2, \ldots, m$. The product ab is now defined as the finite sequence $s = (s_1, \ldots, s_m)$, where $s_1 \equiv (a_1 b_1) \mod q$ and $s_j \equiv (a_1 b_j + a_2 b_{j-1} + \cdots + a_j b_a + d_j) \mod q$ for $j \geq 2$. Here one assumes $a_j = 0$ for $j = k+1, \ldots, m$, and, $b_j = 0$ for $j = l+1, \ldots, m$. See Section 3.4 for worked examples of an addition and a multiplication.

With this addition and multiplication, the $\mathbf{GBT}_n$ is made into a commutative ring with unity [15]. (The multiplicative identity is the sequence $a = (1)$.) These operations can be extended in the most natural way to make the $\mathbf{EGBT}_n$ into a ring. That is, if $a = (a_1, a_2, \ldots)$ and $b = (b_1, b_2, \ldots)$ are from $\mathbf{EGBT}_n$, then the entries for the sum $a + b = (r_1, r_2, \ldots)$ and the product $ab = (s_1, s_2, \ldots)$ are given by the same rules as in the $\mathbf{GBT}_n$. The $\mathbf{EGBT}_n$ is also a commutative ring with unity $a = (1, 0, 0, \ldots)$ [15].

Let x and y be be any two elements in $\mathbf{Z}/(q)$ and denote $B_q(x)$ by $x_n \ldots x_0$ and $B_q(y)$ by $y_n \ldots y_0$. Let $C(x, y)$ be the carry of $x + y$ and denote $B_q(C(x, y))$ by $C_n(x, y) \ldots C_0(x, y)$.

LEMMA 3.2.6. *If there is a carry of 1 from the i^{th} position of the binary sum of $x_n \ldots x_0$ and $y_n \ldots y_0$, then $C_i(x, y) = 1$; if there is a carry of 0, then $C_i(x, y) = 0$.*

PROOF: If we add $x_n \ldots x_0$ and $y_n \ldots y_0$, then for $(i+1)^{th}$ position we have $r_{i+1} = (x_{i+1} + y_{i+1} + c_i) \mod 2$, where c_i is the carry from the i^{th} position.(Notice that since we use modulo $p = 2^{n+1} - 1$, the carry from the n^{th} position will go to the 0^{th} position.) Let $r_n \ldots r_0$ denote $B_q(r)$ and let $z_n \ldots z_0$ denote $E(B_q(x), B_q(y), B_q(r))$. If $c_i = 0$, we have the following four cases:

	case 1	case 2	case 3	case 4
$x_{i+1} =$	0	0	1	1
$y_{i+1} =$	0	1	0	1
$r_{i+1} =$	0	1	1	0
$z_{i+1} =$	0	0	0	0.

If $c_i = 1$, we have the following four cases:

	case 1	case 2	case 3	case 4
$x_{i+1} =$	0	0	1	1
$y_{i+1} =$	0	1	0	1
$r_{i+1} =$	1	0	0	1
$z_{i+1} =$	1	1	1	1.

From all the possible cases we conclude that the *exclusive or* $z_n...z_{i+1}...z_0$ has a 1 in the $(i+1)^{th}$ position. (i.e. $z_{i+1} = 1$, if and only if $c_i = 1$.) Since $C_n(x,y)...C_0(x,y) = T^{-1}(z_n...z_0)$, we have $C_n(x,y) = z_0$, $C_{n-1}(x,y) = z_n$, ..., $C_i(x,y) = z_{i+1}$, ..., $C_0(x,y) = z_1$. Therefore, $C_i(x,y) = 1$ if and only if $c_i = 1$.□

LEMMA 3.2.7. *Let x and y be any two elements in $\mathbf{Z}/(q)$. Let $u_n...u_0$ denote $T^i(B_q(x))$ and $v_n...v_0$ denote $T^i(B_q(y))$. Let u denote $B_q^{-1}(u_n...u_0)$ and v denote $B_q^{-1}(v_n...v_0)$. If $C_n(x,y)...C_0(x,y)$ denotes $B_q(C(x,y))$ and $C_n(u,v)...C_0(u,v)$ denotes $B_q(C(u,v))$, then $C_i(x,y) = C_n(u,v)$.*

PROOF: Since the carry $C_n(x,y)...C_0(x,y)$ of $B_q(x) + B_q(y)$ is circular, the carry $C_n(u,v)...C_0(u,v)$ of $B_q(u) + B_q(v)$ is $T^i(C_n(x,y)...C_0(x,y))$. Therefore, $C_n(u,v) = C_i(x,y)$.□

LEMMA 3.2.8. *If x is a fixed element in $\mathbf{Z}/(q)$ and $B_q(C(x,y))$ is denoted by $C_n(x,y)...C_0(x,y)$ for each element y in $\mathbf{Z}/(q)$, then there are $x-1$ digits $y \in \mathbf{Z}/(q)$ such that $C_n(x,y) = 1$.*

PROOF: Let x be a fixed element in $\mathbf{Z}/(q)$. If $y \in \mathbf{Z}/(q)$ and $y > q - x$, then $x + y > q$. Thus, $B_q(x) + B_q(y)$ has a carry of 1 from the n^{th} position. By Lemma 3.2.6, $C_n(x, y) = 1$. Since y is less than or equal $q - 1$, there are $x - 1$ choices for y such that $C_n(x, y) = 1$.□

LEMMA 3.2.9. *If x is an element in $\mathbf{Z}/(q)$ and $B_q(C(x, y))$ is denoted by $C_n(x, y)...C_0(x, y)$ for each y in $\mathbf{Z}/(q)$, then there are $u - 1$ digits $y \in \mathbf{Z}/(q)$ such that $C_i(x, y) = 1$, where $u = B_q^{-1}(T^i(B_q(x)))$.*

PROOF: Let $u_n...u_0$ equal $T^i(B_q(x))$ and $v_n...v_0$ equal $T^i(B_q(y))$. Let u denote $B_q^{-1}(u_n...u_0)$ and v denote $B_q^{-1}(v_n...v_0)$. Let $C_n(x, y)...C_0(x, y)$ denote $B_q(C(x, y))$ and $C_n(u, v)...C_0(u, v)$ denote $B_q(C(u, v))$. By Lemma 3.2.7, $C_i(x, y) = C_n(u, v)$. By Lemma 3.2.8, there are $u - 1$ digits $v \in \mathbf{Z}/(q)$ such that $C_n(u, v) = 1$. Therefore, there are $u - 1$ digits $y \in \mathbf{Z}/(q)$ such that $C_i(x, y) = 1$.□

PROPOSITION 3.2.10. *If $x \in \mathbf{Z}/(q)$, then $C(x, 0) + C(x, 1) + ... + C(x, q - 1) = [(n + 1)x2^n] \mod q$.*

PROOF: Let $\bar{x}_0 = x$, $\bar{x}_1 = B_q^{-1}(T(B_q(x)))$, $\bar{x}_2 = B_q^{-1}(T^2(B_q(x)))$, ..., $\bar{x}_n = B_q^{-1}(T^n(B_q(x)))$. Notice that $\bar{x}_1 = 2x \mod q$, $\bar{x}_2 = 2^2x \mod q$, ..., $\bar{x}_n = 2^n x \mod q$. Consider the binary sequences $B_q(C(x, 0)), B_q(C(x, 1)), ..., B_q(C(x, q - 1))$. By Lemma 3.2.9, there are $\bar{x}_0 - 1$ digits $j \in \mathbf{Z}/(q)$ such that $C_n(x, j) = 1$. There are $\bar{x}_1 - 1$ digits $j \in \mathbf{Z}/(q)$ such that $C_{n-1}(x, j) = 1$, ..., and there are $\bar{x}_n - 1$ digits $j \in \mathbf{Z}/(q)$ such that $C_0(x, j) = 1$, where $j = 0, ..., q - 1$. Therefore, the sum of the carries $C(x, 0)$, $C(x, 1)$, ..., $C(x, q - 1)$ denoted by $[\sum_{y=1}^{q-1} C(x, y)] \mod q$ can be calculated by the following sequence of equalities.

$$[\sum_{y=1}^{q-1} C(x,y)] \mod q = \{[(\bar{x}_0 - 1)2^n] \mod q + ... + [(\bar{x}_n - 1)] \mod q\} \mod q$$

$$= [(\bar{x}_0 - 1)2^n + (\bar{x}_1 - 1)2^{n-1} + ... + (\bar{x}_{n-1} - 1)2 + (\bar{x}_n - 1)] \mod q$$

$$= [(x-1)2^n + (2x-1)2^{n-1} + ... + (2^{n-1}x - 1)2 + (2^n x - 1)] \mod q$$

$$= [(\underbrace{x2^n + ... + x2^n}_{n+1}) - (2^n + 2^{n-1} + ... + 2 + 1)] \mod q$$

$$= [(n+1)x2^n - (2^{n+1} - 1)] \mod q$$

$$= [(n+1)x2^n] \mod q.\square$$

COROLLARY 3.2.11. *If $x = 1$, then $[\sum_{y=1}^{q-1} C(x,y)] \mod q = [(n+1)2^n] \mod q$.*

PROPOSITION 3.2.12. *If x is an element in $\mathbf{Z}/(q)$ relatively prime to q, let $\mathcal{F}(\underbrace{x,...,x}_{q})$ denote the carry of the result of adding the element x to itself p times, then the carry $\mathcal{F}(\underbrace{x,...,x}_{q})$ equals $[x(n+1)2^n] \mod q$.*

PROOF: Since $\mathcal{F}(\underbrace{x,...,x}_{q}) = C(x,x) + C(2x \mod q, x) + ... + C((q-1)x \mod q, x)$, and $(mx) \mod q \neq (lx) \mod q$ if $m \neq l$, where $0 < l, m < q$, $\mathcal{F}(\underbrace{x,...,x}_{q}) = [C(x,1) + C(x,2) + ... + C(x,q-1)] \mod q = [\sum_{y=1}^{q-1} C(x,y)] \mod q$. By Proposition 3.2.10, $\mathcal{F}(\underbrace{x,...,x}_{q}) = [x(n+1)2^n] \mod q.\square$

COROLLARY 3.2.13. *If we add the digit one p times, then the carry $\mathcal{F}(\underbrace{1,...,1}_{p})$ equals $[(n+1)2^n] \mod q$.*

§3.3. The ring $\mathbf{EGBT}_n$ and q-adic integers

The ring $\mathbf{EGBT}_n$ is the set $\{(a_1, a_2, a_3, ...) : 0 \leq a_k < q\}$ with addition and multiplication as defined in Section 3.2 [15]. It can be shown that the subset I_k of $\mathbf{EGBT}_n$ defined by $I_k = \{(\underbrace{0, ..., 0}_{k}, x_{k+1}, x_{k+2}, ...) : x_i \in \mathbb{Z}/(q)\}$ is an ideal of $\mathbf{EGBT}_n$.

PROPOSITION 3.3.1. *For each positive integer k the cardinality of $\mathbf{EGBT}_n/I_k$ is q^k.*

PROOF: Let $q = 2^{n+1} - 1$. The set $\mathbf{EGBT}_n = \{(a_1, a_2, ..., a_k, 0...) + I_k : a_i \in \mathbb{Z}/(q)$ for all $i = 1, 2, ...\}$. Since there are q choices for each a_i in each of the first k components, there are q^k choices for $(a_1, a_2, ..., a_k, 0, ...) + I_k$. Therefore, the cardinality of $\mathbf{EGBT}_n/I_k$ is q^k.□

Note: In the following lemmas and propositions an arbitrary value will be denoted by the symbol *. It may be the case that * will represent one value on one side of an equation or expression and another on the other side.

LEMMA 3.3.2. *Let x be an element in $\mathbb{Z}/(q)$ which is relatively prime to q. If $n+1$ and q are relatively prime, then the following relation holds in the ring $\mathbf{EGBT}_n$.*

$$\underbrace{(x,*) + ... + (x,*)}_{l} = \begin{cases} (0, x_2, *), & \text{if } l = q, \text{ where } x_2 = [x(n+1)2^n] \mod q \\ & \text{and } gcd(x_2, q) = 1; \\ (x_1, *), & \text{if } l < p, \text{ where } x_1 \text{ is a nonzero element in } \mathbb{Z}/(q). \end{cases}$$

In particular,

$$\underbrace{(1,*) + ... + (1,*)}_{l} = \begin{cases} (0, x_2, *), & \text{if } l = q, \text{where } x_2 = [(n+1)2^n] \mod q \\ (l, *), & \text{if } l < q \end{cases}.$$

PROOF: If $l = q$, then $(x,*)+...+(x,*) = ((qx) \mod q, \mathcal{F}(\underbrace{x, ..., x}_{q}, *) = (0, \mathcal{F}(\underbrace{x, ..., x}_{q}, *)$. By Lemma 3.2.12, $\mathcal{F}(\underbrace{x, ..., x}_{q}) = [x(n+1)2^n] \mod q$. Since x and $n+1$ are both rela-

tively prime to q, $x(n+1)2^n$ is relatively prime to q. Therefore, $\underbrace{(x,*)+\ldots+(x,*)}_{q} = (0,x_2,*)$, where $x_2 = [x(n+1)2^n] \mod q$ and x_2 is relatively prime to q. If $l < q$, then $\underbrace{(x,*)+\ldots+(x,*)}_{l} = ((lx) \mod q,*)$. Since x and q are relative prime and $l < q$, $(lx) \mod q \neq 0$. If x_1 denotes $(lx) \mod q$, then we have $\underbrace{(x,*)+\ldots+(x,*)}_{l} = (x_1,*)$, where $x_1 \neq 0$.□

LEMMA 3.3.3. *If $n+1$ and q are relatively prime, and if $l = q^k$ for some positive integer k, then $\underbrace{(1,*)+\ldots+(1,*)}_{l} = (\underbrace{0,\ldots,0}_{k},x_{k+1},*)$, where x_{k+1} is relatively prime to q and $x_{k+1} = [(n+1)2^n]^k \mod q$.*

PROOF: The proof will be by induction on the integer k.

If $k = 1$, (i.e. $l = q$), then by Lemma 3.3.2, $\underbrace{(1,*)+\ldots+(1,*)}_{l=q}=(0,x_2,*)$, where $x_2 = [(n+1)2^n] \mod q$. By assumption, x_2 is relatively prime to q. Therefore, the inductive step is true for $k = 1$.

Assume that the inductive step is true for all integers less than or equal k.

By the inductive assumption, we have $\underbrace{(1,*)+\ldots+(1,*)}_{q^k}=(\underbrace{0,\ldots,0}_{k},x_{k+1},*)$, where x_{k+1} is relatively prime to q and $x_{k+1} = [(n+1)2^n]^k \mod q$.

If $l = q^{k+1}$, then by Lemma 3.3.2

$$\underbrace{(1,*)+\ldots+(1,*)}_{q^{k+1}} = \underbrace{\underbrace{(1,*)+\ldots+(1,*)}_{q^k}+\ldots+\underbrace{(1,*)+\ldots+(1,*)}_{q^k}}_{q}$$

$$= \underbrace{(\underbrace{0,...,0}_{k}, x_{k+1}, *) + ... + (\underbrace{0,...,0}_{k}, x_{k+1}, *)}_{q}$$

$$= (\underbrace{0,...0}_{k+1}, x_{k+2}, *),$$

where $x_{k+2}=[x_{k+1}(n+1)2^n] \mod q$.

Since the integers x_{k+1} and $(n+1)2^n$ are both relatively prime to q, x_{k+2} is relatively prime to q, and $x_{k+2} = \{[(n+1)2^n]^k(n+1)2^n\} \mod q = [(n+1)2^n]^{k+1} \mod q$. Therefore, the induction is true for the integer $k+1$.□

LEMMA 3.3.4. *If $n+1$ and q are relatively prime, and if $l = q^k$, then* $\underbrace{(1,*) + ... + (1,*)}_{l} = (\underbrace{0,...,0}_{k}, x_{k+1}, *)$, *where x_{k+1} is relative prime to q. If $l < q^k$, then* $\underbrace{(1,*) + ... + (1,*)}_{l} = (x_1, ..., x_k, *)$, *where x_i is a nonzero element in $\mathbb{Z}/(q)$ for some integer i between 1 and k.*

PROOF: The proof will be by induction on integer k.

If $k = 1$, then by Lemma 3.3.2 $\underbrace{(1,*) + ... + (1,*)}_{l} = (0, x_2, *)$ for $l = q$, where x_2 is relatively prime to q. Also, if $l < q$, then $\underbrace{(1,*) + ... + (1,*)}_{l} = (x_1, *)$, where x_1 is a nonzero element in $\mathbb{Z}/(q)$.

Assume that the inductive step is true for all integers less than or equal k (i.e. $l \leq q^k$).

If $l = q^{k+1}$, then by Lemma 3.3.3

$$\underbrace{(1,*) + ... + (1,*)}_{l} = (\underbrace{0,...0}_{k+1}, x_{k+2}, *), \text{ where } x_{k+2} \text{ is relatively prime to } q.$$

If $l < q^{k+1}$ (i.e. $l = hq^k + l'$ where $h < q$ and $l' < q^k$), then by Lemma 3.3.2 we have

$$\underbrace{(1,*)+...+(1,*)}_{l} = \underbrace{(1,*)+...+(1,*)}_{hq^k} + \underbrace{(1,*)+...+(1,*)}_{l'}$$

$$= \underbrace{\underbrace{(1,*)+...+(1,*)}_{p^k} + ... + \underbrace{(1,*)+...+(1,*)}_{q^k}}_{h} + \underbrace{(1,*)+...+(1,*)}_{l'}$$

$$= \underbrace{(\underbrace{0,...,0}_{k}, x_{k+1}, *) + ... + (\underbrace{0,...,0}_{k}, x_{k+1}, *)}_{h} + \underbrace{(1,*)+...+(1,*)}_{l'}$$

$$= (\underbrace{0,...,0}_{k}, (hx_{k+1}) \mod q, *) + \underbrace{(1,*)+...+(1,*)}_{l'}.$$

By the induction assumption we have $\underbrace{(1,*)+...+(1,*)}_{l'} = (x_1, x_2, ..., x_k, *)$, where some x_i is a nonzero element in $\mathbf{Z}/(q)$ if and only if l' is different from zero.

Thus, if $l' \neq 0$, then, by induction, there is an integer $i \leq k$ such that x_i is a nonzero element in $\mathbf{Z}/(q)$. If $l' = 0$, then by induction, x_{k+1} is relatively prime to q. Since $h < q$, $(hx_{k+1}) \mod q \neq 0$. Therefore, the induction is true for the integer $k+1$.□

PROPOSITION 3.3.5. *If $n+1$ and q are relatively prime, then the ring $\mathbf{EGBT}_n/I_k$ is generated (under addition) by the element $\bar{1}_k = (1,0,0,...) + I_k \in \mathbf{EGBT}_n/I_k$.*

PROOF: By Lemma 3.3.4, we have:

$$\underbrace{\bar{1}_k + ...\bar{1}_k}_{l} = \underbrace{(1,0,0,...) + I_k + ... + (1,0,0,...) + I_k}_{l}$$

$$= \underbrace{(1,0,0,...) + ... + (1,0,0,...)}_{l} + I_k$$

$$= \begin{cases} (\underbrace{0,...0}_{k}, x_{k+1}, *) + I_k, & \text{if } l = q^k \\ (x_1, ..., x_k, *) + I_k, & \text{if } l < q^k, \text{ where } x_i \in \mathbf{Z}/(q), x_i \neq 0 \text{ for some i}\in\{1,..k\}. \end{cases}$$

Thus, $\underbrace{\bar{1}_k + ... + \bar{1}_k}_{l} = I_k$ if and only if $l = p^k$. Therefore, the order of $\bar{1}_k$ is q^k. By Proposition 3.3.1, $\bar{1}_k$ is the generator of $\mathbf{EGBT}_n/I_k$ under addition.□

THEOREM 3.3.6. *If $n+1$ and q are relatively prime, where $q = 2^{n+1} - 1$, then the ring $\mathbf{EGBT}_n$ is isomorphic to the ring of q-adic integers.*

PROOF: By Proposition 3.3.1 we know that $\mathbf{EGBT}_n/I_k$ has order q^k for all positive integers k. By Proposition 3.3.5, if $n+1$ and q are relatively prime, then $\mathbf{EGBT}_n/I_k$ is generated (under addition) by $\bar{1}_k$ for all positive integers k. Thus, by Corollary 2.2.4 $\{\mathbf{EGBT}_n/I_k (k = 1, 2, ...); \phi_k^l\}$ is an inverse system, and $\mathbf{EGBT}_n^* = \varprojlim(\mathbf{EGBT}_n/I_k; \phi_k^l)$ is isomorphic to $\mathbf{Z}_q$.It is easy to show that $\mathbf{EGBT}_n = \{((x_1, 0, ...) + I_1, (x_1, x_2, 0, ...) + I_2, ...); x_k \in \mathbf{Z}/(q)$ for $k = 1, 2, ...\}$.

Now if we define the function $\eta : \mathbf{EGBT}_n \mapsto \mathbf{EGBT}_n^*$ by $\eta(x_1, x_2, ...) = ((x_1, 0, ...) + I_1, (x_1, x_2, 0, ...) + I_2, ...)$ for all $(x_1, x_2, ...) \in \mathbf{EGBT}_n$. It can be proved in a way similar to the proof in Proposition 2.3.9 that η is an isomorphism from $\mathbf{EGBT}_n$ to $\mathbf{EGBT}_n^*$. Since $\mathbf{EGBT}_n^*$ is isomorphic to $\mathbf{Z}_q$, we have that $\mathbf{EGBT}_n$ is isomorphic to $\mathbf{Z}_q$.□

COROLLARY 3.3.7. *If $n+1$ is prime, then the ring $\mathbf{EGBT}_n$ is isomorphic to the ring of q-adic integers, where $q = 2^{n+1} - 1$.*

For the case when $n+1$ and $q = 2^{n+1} - 1$ are not relative prime, this proof can not be used to establish the existence of the isomorphism.

§3.4. Examples

In this section some examples are given which illustrates that the addition and multiplication operations between the addresses can be carried out using simple operations on bit strings.

EXAMPLE 3.4.1.

In 3-dimensional space, $q = 15$, the sum of the addresses $a = (6) = (0110)$ and $b = (12) = (110)$ has remainder r. Here, $r_1 = (6 + 12) \mod 15 = 3 = 0011$. The carry $c_2 = C(6,12) = B_q^{-1}(T^{-1}(E(0110,1100,0011))) = B_q^{-1}(T^{-1}(1001)) = B_q^{-1}(1100) = 12$. Thus, $r_2 = 0 + 0 + 12 = 12$. Therefore, the sum of the addresses a and b is $r = (r_1, r_2) = (3, 12)$.

EXAMPLE 3.4.2.

The product of the addresses $a = (6) = (0110)$ and $b = (3) = (0011)$ in 3-dimensional space has remainder s. Here, $s_1 = (6 \times 3) \mod 15 = 3 = 0011$. Since $3 = 2 + 1$, $D(6,3) = C((6 \times 2) \mod 15, 6) = C(12,6)$. From Example 3.4.1, $C(12,6) = 12$. The carry $d_2 = D(6,3) = C(12,6) = 12 = 1100$. Thus, $s_2 = 6 \times 0 + 0 \times 3 + 12 = 12$. Therefore, the product of the addresses a and b is $s = (3, 12)$.

CHAPTER 4
ANOTHER APPROACH TO $\mathbf{EGBT_n}$ AND THE $\mathbf{q-adic}$ INTEGERS

§4.1. Introduction

The material presented in this section is a modification of the material described by A. Vince [12, Section 3].

Let α be an arbitrary element of a ring R and consider the inverse system

$$R/\alpha R \xleftarrow{f_1} R/\alpha^2 R \xleftarrow{f_2} \dots \xleftarrow{f_{k-1}} R/\alpha^k R \xleftarrow{f_k} \dots, \tag{1}$$

where the ring homomorphisms f_k are defined so that $f_k(\overline{\beta})$ is equal to the equivalence class of $\beta \pmod{\alpha^k}$. The *inverse limit* $\mathbf{R}_\alpha$ of this system consists of all sequences $\{\overline{\beta}_0, \overline{\beta}_1, \dots\}$ such that $f_k(\overline{\beta}_k) = \overline{\beta}_{k-1}$. The definition and notation is analogous to that of the p-adic integers $\mathbf{Z}_p$. Addition and multiplication in $\mathbf{R}_\alpha$ are defined in the usual manner for inverse systems. If $\{\overline{\beta}_0, \overline{\beta}_1, \dots\}$ is an element in $\mathbf{R}_\alpha$ and S is a set of coset representatives for $R/\alpha R$, then it follows from the definition of the homomorphisms f_k that there exists a unique sequence $(s_0, s_1, s_2 \dots)$ of elements of S such that

$$\beta_0 \equiv s_0 \pmod{\alpha}$$

$$\beta_1 \equiv s_0 + s_1\alpha \pmod{\alpha^2}$$

$$\dots$$

$$\beta_k \equiv s_0 + s_1\alpha + \dots + s_k\alpha^k \pmod{\alpha^{k+1}}$$

$$\dots.$$

The element $s_0 + s_1\alpha + s_2\alpha^2 + \ldots$ in $\mathbf{R}_\alpha$ will be abbreviated $(s_0 s_1 s_2 \ldots)$, where α is understood.

Let n be a positive integer and consider the special case where R is the quotient ring

$$R = \mathbb{Z}[x]/(f),$$

with $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Let $\omega = x + (f)$, the coset containing x. Note that $f(\omega) = 0$. As a free abelian group, R has basis $\{1, \omega, \ldots, \omega^{n-1}\}$. Vince [28] discussed the ring structure of R and indicated that R can be realized as a lattice in $\mathbb{R}^n$ by embedding the n basis elements as n linearly independent vectors in $\mathbb{R}^n$. In Section 4.2, we will discuss the algebraic structure of $\mathbf{R}_\alpha$, where $\alpha = \overline{l} - \omega$ and l is a non-zero integer.

When one chooses $f(x) = x^n + x^{n-1} + \cdots + x + 1$ and $\alpha = \overline{2} - \omega$, $\mathbf{R}_\alpha$ is isomorphic to $\mathbf{EGBT}_n$ as defined in Chapter 3. The isomorphism ϕ is defined as follows. Vince has shown that the set $\mathcal{S} = \{\epsilon_0 + \epsilon_1\omega + \cdots + \epsilon_n\omega^n : \epsilon_i \in \{0,1\}$, not all $\epsilon_i = 1\}$ is a set of coset representatives for $R/\alpha R$ [12]. Thus, any element $s \in \mathbf{R}_\alpha$ can be expresed as $s = s_0 + s_1\alpha + s_2\alpha^2 + \ldots$, where $s_i = \sum_{j=0}^{n} \epsilon_j^i \omega^j \in \mathcal{S}$, $i = 0, 1, \ldots$ and $\epsilon_j^i \in \{0,1\}$. Recall from Chapter 3 that the elements $a \in \mathbf{EGBT}_n$ are infinite sequences $(a_0, a_1, a_2, \ldots)$, where a_i is an integer from the set $\{0, \ldots, q-1\}$, $q = 2^{n+1} - 1$. Define a map ϕ from $\mathbf{R}_\alpha$ to $\mathbf{EGBT}_n$ by $\phi(s) = (a_0, a_1, a_2, \ldots)$, where $a_i = \sum_{j=0}^{n} \epsilon_j^i 2^i$. Clearly ϕ is a bijection from $\mathbf{R}_\alpha$ onto $\mathbf{EGBT}_n$.

That $\phi(s + t) = \phi(s) + \phi(t)$, where $s, t \in \mathbf{R}_\alpha$, can be seen as follows. Let $s_i = \sum_{j=0}^{n} \epsilon_j^i \omega^j$ and $t_i = \sum_{j=0}^{n} \eta_j^i \omega^j$ be two elements from $\mathcal{S}$. Use the fact that $2 = \omega + \alpha$ and $\omega^{n+1} \equiv 1 \mod (\omega^n + \omega^{n-1} + \cdots + \omega + 1)$ to express $s_i + t_i$ as $v_i + w_i\alpha$. This is done formally as follows:

Define $u_i = \sum_{j=0}^{n+1} \delta_j^i \omega^j$ by the following rules

$$\delta_0^i = (\epsilon_0^i + \eta_0^i) \mod 2,$$
$$\delta_j^i = (\epsilon_j^i + \eta_j^i + \sigma_j^i) \mod 2, j = 1, \ldots, n+1,$$

where $\sigma_0^i = 0$, $\sigma_j^i = 1$ if and only of $\epsilon_{j-1}^i + \eta_{j-1}^i + \sigma_{j-1}^i \geq 2$ and $\epsilon_{n+1}^i = 0 = \eta_{n+1}^i$. For example, $s_i = 1 + \omega$ added to $t_i = \omega + \omega^2$ yields $u_i = 1 + \omega^3$. Now define

$$v_i = \sum_{j=0}^{n} \beta_j^i \omega^j,$$
$$u_i = (\gamma_1^i + \gamma_2^i \omega + \gamma_3^i \omega^2 + \cdots + \gamma_n^i \omega^{n-1} + \gamma_0^i \omega^n)\alpha$$

by the following rules.

$$\beta_0^i = (\epsilon_0^i + \eta_0^i + \gamma_0^i) \mod 2,$$
$$\beta_j^i = (\epsilon_j^i + \eta_j^i + \gamma_j^i) \mod 2, j = 1, \ldots, n,$$

where $\gamma_0^i = \delta_{n+1}^i$, and $\gamma_j^i = 1$ if and only if $\epsilon_{j-1}^i + \eta_{j-1}^i + \gamma_{j-1}^i \geq 2$. If $s = s_0 + s_1\alpha + \cdots + s_i\alpha^i + \ldots$ and $t = t_0 + t_1\alpha + \cdots + t_i\alpha^i + \ldots$ are elements of $\mathbf{R}_\alpha$, then $a_i = \sum_{j=0}^{n} \epsilon_j^i 2^j$ and $b_i = \sum_{j=0}^{n} \eta_j^i 2^j$ are the entries in the sequences $\phi(s)$ and $\phi(t)$. It can be checked that the definition in Chapter 3 used to define the sum $a_i + b_i$ corresponds exactly to the definition for $s_i + t_i = v_i + w_i\alpha$. In other words, the remainder and carry rules are preserved under the map ϕ. This implies that $\phi(s+t) = \phi(s) + \phi(t)$. To convince oneself that $\phi(st) = \phi(s)\phi(t)$ takes a little more work and is left to the reader.

§4.2. The Structure of $\mathbf{R}_\alpha$

The material presented in this section is a generalization of the results presented by Vince [12,Section 4].

The q-adic integers $\mathbf{Z}_q$ are defined as the inverse limit of the inverse system

$$\mathbf{Z}/q\mathbf{Z} \xleftarrow{g_1} \mathbf{Z}/q^2\mathbf{Z} \xleftarrow{g_2} \ldots \xleftarrow{g_{k-1}} \mathbf{Z}/q^k\mathbf{Z} \xleftarrow{g_k} \ldots,$$

where the homomorphisms g_k take an integer j (mod q^{k+1}) to the integer j (mod q^k). If $f(x)$ is any monic polynomial, we have the following lemmas which lead us to an isomorphism between $\mathbf{R}_\alpha$ and $\mathbf{Z}_q$.

LEMMA 4.2.1. *If R is a ring, $\alpha \in R$ and $S \subset R$ is a set of coset representatives of $R/\alpha R$, then*

$$S \oplus \alpha S \oplus \cdots \oplus \alpha^{k-1} S \subset R$$

is a set of coset representatives of $R/\alpha^k R$.

PROOF: Since S is a set of coset representatives of $R/\alpha R$

$$\begin{aligned} R &= S \oplus \alpha R = S \oplus \alpha(S \oplus \alpha R) = S \oplus \alpha S \oplus \alpha^2 R \\ &\vdots \\ &= S \oplus \alpha S \oplus \alpha^2 S \oplus \cdots \oplus \alpha^{k-1} S \oplus \alpha^k R. \square \end{aligned}$$

LEMMA 4.2.2. *If m is any integer, then $\overline{m}$ is divisible by α in $R = \mathbb{Z}[x]/f(x)$ if and only if m is divisible by $q = f(l)$ in $\mathbb{Z}$, where $l \in \mathbb{Z}$, $\alpha = \overline{l} - \omega$ and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.*

PROOF: Let $q = f(l) = l^n + a_{n-1}l^{n-1} + \cdots + a_1 l + a_0$ and suppose m is divisible by q. Let $g(x) = f(l - x)$. Since $g(\alpha) = g(l - \omega) = f(\omega) = 0$,

$$0 = g(\alpha) = \sum_{i=0}^{n} a_i (l - \alpha)^i = q - \alpha h(\alpha),$$

where $a_n = 1$ and $h(x)$ is some polynomial in $\mathbf{Z}[x]$. The above equation implies that q is divisible by α. Therefore, since m is divisible by q, $\overline{m}$ is divisible by α.

Conversely, suppose $\overline{m}$ is divisible by α. Note that for any $\overline{a} \in R$, $\overline{a} = g(\omega)$, for some $g(x) \in \mathbf{Z}[x]$. Since $\alpha = \overline{l} - \omega$, if we let $h_1(x) = g(l - x)$, $h_1(x) \in \mathbf{Z}[x]$, then we have $h_1(\alpha) = g(\overline{l} - \alpha) = g(\omega) = \overline{a}$. Since α divides $\overline{m}$, $\overline{m} = \alpha\overline{a}$, for some $\overline{a} \in R$. But $\overline{a} = h_1(\alpha)$, for some $h_1(x) \in \mathbf{Z}[x]$. Therefore, $\overline{m} = \alpha h_1(\alpha)$, for some $h_1(x) \in \mathbf{Z}[x]$. Let $k_1(x) = x h_1(x) - m$. Let d be the greatest common divisor of the coefficients of $k_1(x)$ and let $k(x) = \frac{1}{d} k_1(x)$. Since $k(\alpha) = 0$ and $g(x)$ is the polynomial of minimum degree in the ring $R = \mathbf{Z}[x]/(f)$ satisfied by α (since $f(x)$ is the polynomial of minimum degree in R such that $f(\omega) = 0$ and $g(x) = f(l - x)$), it must be the case that $k(x) = g(x)q(x)$, where $q(x) \in \mathbf{Q}[x]$. Since the greatest common divisor of the coefficients of $k(x)$ (and also of $g(x)$) is 1, it follows that $q(x) \in \mathbf{Z}[x]$. The constant terms in $k(x)$ and $g(x)$ are $\frac{m}{d}$ and q, respectively. Therefore, since q divides $\frac{m}{d}$, q divides m. □

Remark. The polynomial $f(x)$ may not be minimal over $\mathbf{Z}[x]$. For example, if $f(x) = x^3 + x^2 + x + 1 = (x^2 + 1)(x + 1)$, then $f(x)$ is not the polynomial with minimum degree such that $f(\omega) = f(\sqrt{-1}) = 0$.

LEMMA 4.2.3. *If* $q = f(l) = l^n + a_{n-1}l^{n-1} + \cdots + a_1 l + a_0$ *and* $\alpha = \overline{l} - \omega$, *then* $|R/\alpha^k R| = q^k$.

PROOF: Lemma 4.2.3 follows from Lemma 4.2.1 once it is shown that $|R/\alpha R| = q$. Since every element of R can be represented by a polynomial in ω with coefficients

in $\mathbb{Z}$, every element of R can be written as a polynomial in α with coefficients in $\mathbb{Z}$. This last fact implies that every element of $R/\alpha R$ can be represented as $\overline{m}$ for some integer m. Now $|R/\alpha R| = q$ follows from Lemma 4.2.2. □

THEOREM 4.2.4. *Let* $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *and* $\alpha = \overline{l} - \omega$, *where* $l \in \mathbb{Z}$. *Let* $q = f(l)$. *If* $f(l)$ *and* $f'(l)$ *are relative prime, then there is a ring isomorphism* $\mathbf{R}_\alpha = \varprojlim R/\alpha^k R \cong \mathbf{Z}_q$.

PROOF: An isomorphism will be constructed by finding *vertical* isomorphisms that make the following diagram commute.

$$\begin{array}{ccccccccc} R/\alpha R & \longleftarrow & R/\alpha^2 R & \longleftarrow & \cdots & \longleftarrow & R/\alpha^k R & \longleftarrow & \cdots \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \mathbb{Z}/q\mathbb{Z} & \longleftarrow & \mathbb{Z}/q^2\mathbb{Z} & \longleftarrow & \cdots & \longleftarrow & \mathbb{Z}/q^k\mathbb{Z} & \longleftarrow & \cdots \end{array}$$

Since each vertical map is to be a ring isomorphism, each of these vertical maps must take the multiplicative identity 1 in $R/\alpha^k R$ to the 1 in $\mathbb{Z}/q^k\mathbb{Z}$. By Lemma 4.2.3 the order of the additive group $R/\alpha^k R$ is q^k. Therefore, these isomorphisms exist if and only if the additive order of the element 1 in $R/\alpha^k R$ is q^k. This fact will be proved by induction on k. The case $k = 1$ is exactly Lemma 4.2.2. By way of induction assume that the order of 1 in $R/\alpha^{k-1}R$ is q^{k-1}. With the polynomial $g(x)$ defined exactly as it was in the proof of Lemma 4.2.2

$$0 = g(\alpha) = \sum_{i=0}^{n} a_i(l-\alpha)^i = q - a\alpha + \alpha^2 h(\alpha),$$

where $a_n = 1$, $h(x) \in \mathbb{Z}[x]$, $q = l^n + a_{n-1}l^{n-1} + \cdots + a_1 l + a_0$ and $a = nl^{n-1} + (n-1)a_{n-1}l^{n-2} + \cdots + 2a_2 l + a_1$. The above equation implies that

$$q^{k-1} = a^{k-1}\alpha^{k-1} + \alpha^k h_1(\alpha) \tag{4}$$

where $h_1(x) \in \mathbb{Z}[x]$. The order of 1 in $R/\alpha^k R$ must be a multiple cq^{k-1} of the order of 1 in $R/\alpha^{k-1}R$. It now suffices to show that q is the least positive integer c such that cq^{k-1} is divisible by α^k. From (4)

$$cq^{k-1} = ca^{k-1}\alpha^{k-1} + c\alpha^k h_1(\alpha).$$

This equation implies that cq^{k-1} is divisible by α^k if and only if ca^{k-1} is divisible by α. By Lemma 4.2.2 this equivalence is the case if and only if ca^{k-1} is divisible by q. Since $gcd(a, q) = 1$ (i.e. $f(l)$ and $f'(l)$ are relative prime), q divides c. Since c is the least such integer, $c = q$. Therefore, the induction is true for the integer k. □

One particular case of Theorem 4.2.4 is when $f(x) = x^n + x^{n-1} + \cdots + x + 1$. In this case, one needs the following lemmas to prove Corollary 4.2.7.

LEMMA 4.2.5. *Let* $q = l^n + l^{n-1} + \cdots + l + 1$ *and let* $a = nl^{n-1} + (n-1)l^{n-2} + \cdots + 2l + 1$. *If* $gcd(n+1, q) = 1$, *then* $gcd(n+1, a) = 1$.

PROOF: Since

$$q = l^n + l^{n-1} + \cdots + l + 1 = (n+1)l^n - (nl^{n-1} + \cdots + 2l + 1)(l-1),$$

we have $q = (n+1)l^n - a(l-1)$. Therefore, if $h|a$ and $h|(n+1)$ for some $h \in \mathbb{Z}$, then $h|q$, i.e., if $gcd(n+1, a) \neq 1$, then $gcd(n+1, q) \neq 1$. Thus, if $gcd(n+1, q) = 1$, then $gcd(n+1, a) = 1$. □

LEMMA 4.2.6. *If* $gcd(n+1, q) = 1$, *then* $gcd(q, a) = 1$.

PROOF: Suppose h is prime and h divides $gcd(q, a)$. Since $q = (n+1)l^n - a(l-1)$, we have $h|(n+1)l^n$. If $h|l$, then $h|q - l^n - l^{n-1} - \cdots - l = 1$, i.e., $h = 1$. This contradicts the fact that h is prime and thus greater than one. Therefore, $h \nmid l$. Since h is prime,

$h \nmid l^n$. Write $n+1 = q_1 \dots q_k$, where q_i is a prime for $i = 1, ..., k$. Thus, we have $h = q_i$ for some $i \in \{1, ..., k\}$. By Lemma 4.2.5, we have $gcd(n+1, a) \geq q_i$ and $gcd(n+1, q) > 1$ for some $i \in \{1, ...k\}$. This fact contradicts the assumption that $gcd(n+1, q) = 1$. □

COROLLARY 4.2.7. *Let $\alpha = \bar{l} - \omega$, where $l \in \mathbb{Z}$ and $q = l^n + l^{n-1} + \cdots + l + 1$. If q and $n+1$ are relatively prime, then there is a ring isomorphism from $\mathbf{R}_\alpha$ into $\mathbb{Z}_q$.*

PROOF: By Lemma 4.2.6 we know that q and $a = nl^{n-1} + (n-1)l^{n-2} + \cdots + 2l + 1$ are relatively prime. Since $q = f(l)$ and $a = f'(l)$, the result follows from Theorem 4.2.4. □

CHAPTER 5

THE MATRIX $\mathbf{A}_\alpha$

Define the vector μ_i from $\mathbb{R}^n$ by

$$\mu_i = (-\frac{x_0}{n}, -\frac{x_1}{n-1}, ..., -\frac{x_{i-1}}{n-i+1}, x_i, 0, ..., 0),$$

where $x_i = (\frac{(n-i)(n+1)}{(n-i+1)n})^{\frac{1}{2}}$, for $i = 0, ..., n$. The set $\{\mu_0, \mu_1, \ldots, \mu_{n-1}\}$ is a basis of $\mathbb{R}^n$ [15]. Denote by $\mathbf{A_n}$ the set of all integer linear combinations of the μ_i's. $\mathbf{A_n}$ is an n-dimensional lattice of $\mathbb{R}^n$ and the elements of $\mathbf{A_n}$ are the centers of the $(n+1)$-permutohedron packing of $\mathbb{R}^n$ mentioned in Chapter 1. The particular vector $\alpha = 2\mu_0 - \mu_1$ from $\mathbf{A_n}$ is at the center of a first level aggregate of the second level aggregate centered at the origin. The vector α defines a linear transformation $\mathbf{A}_\alpha$ from $\mathbb{R}^n$ into $\mathbb{R}^n$ given by $\mathbf{A}_\alpha(x) = x\alpha$. The linear transformation $\mathbf{A}_\alpha$ maps the centers of the k^{th} level aggregates onto the centers of $(k+1)^{th}$ level aggregates, where $k = 0, 1, \ldots$. Relative to the ordered basis $\{\mu_0, \mu_1, \ldots, \mu_{n-1}\}$, the linear transformation $\mathbf{A}_\alpha$ is represented by the $n \times n$ matrix

$$\begin{pmatrix} 2 & 0 & 0 & \ldots & 0 & 1 \\ -1 & 2 & 0 & \ldots & 0 & 1 \\ 0 & -1 & 2 & \ldots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 2 & 1 \\ 0 & 0 & 0 & \ldots & -1 & 3 \end{pmatrix}_{n \times n}.$$

By abuse of notation, this matrix will also be called $\mathbf{A}_\alpha$.

D. Wilson suggested that the author investigate the matrix $\mathbf{A}_\alpha$ more closely. In this chapter some of the properties of $\mathbf{A}_\alpha$ are presented.

§5.1. The Algebraic Properties of the Matrix $\mathbf{A}_\alpha$

Since there are $2^{n+1}-1$ cells in the first level aggregate and $(2^{n+1}-1)(2^{n+1}-1)$ cells in the second level aggregate, the volume "stretching factor" is $2^{n+1}-1$. This fact is expressed algebraically in the next proposition.

PROPOSITION 5.2.1. $det(\mathbf{A}_\alpha) = 2^{n+1} - 1$.

PROOF: The proof will be by induction on the size n of the matrix A.

If $n = 2$,

$$\mathbf{A}_\alpha = \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} = 7 = 2^3 - 1$$

Therefore, the inductive step is true for $n = 2$.

Assume that the inductive step is true for all integers less than or equal k.

If $n = k + 1$, then

$$\mathbf{A}_\alpha = \begin{pmatrix} 2 & 0 & 0 & \dots & 0 & 1 \\ -1 & 2 & 0 & \dots & 0 & 1 \\ 0 & -1 & 2 & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2 & 1 \\ 0 & 0 & 0 & \dots & -1 & 3 \end{pmatrix}_{(k+1)\times(k+1)}$$

$$= 2 \times \begin{pmatrix} 2 & 0 & 0 & \dots & 0 & 1 \\ -1 & 2 & 0 & \dots & 0 & 1 \\ 0 & -1 & 2 & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2 & 1 \\ 0 & 0 & 0 & \dots & -1 & 3 \end{pmatrix}_{k \times k} + (-1)^{1+k+1} \times \begin{pmatrix} -1 & & \\ & \ddots & \\ & & -1 \end{pmatrix}_{k \times k}$$

Thus,

$$det(\mathbf{A}_\alpha) = 2 \times (2^{k+1} - 1) + (-1)^{k+2} \times (-1)^k = 2^{k+2} - 1$$

Therefore, the induction is true for the integer $k + 1$. □

PROPOSITION 5.2.2. *Let $P_n(\lambda)$ be the characteristic polynomial of the $n \times n$ matrix $\mathbf{A}_\alpha$, then $P_n(\lambda) = (2 - \lambda)P_{n-1}(\lambda) + 1 = (2 - \lambda)^n + (2 - \lambda)^{n-1} + \dots + (2 - \lambda) + 1$.*

PROOF:

$$P_n(\lambda) = det \begin{pmatrix} 2-\lambda & 0 & 0 & \dots & 0 & 1 \\ -1 & 2-\lambda & 0 & \dots & 0 & 1 \\ 0 & -1 & 2-\lambda & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2-\lambda & 1 \\ 0 & 0 & 0 & \dots & -1 & 3-\lambda \end{pmatrix}_{n \times n}$$

$$= (2 - \lambda) det \begin{pmatrix} 2-\lambda & 0 & 0 & \dots & 0 & 1 \\ -1 & 2-\lambda & 0 & \dots & 0 & 1 \\ 0 & -1 & 2-\lambda & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2-\lambda & 1 \\ 0 & 0 & 0 & \dots & -1 & 3-\lambda \end{pmatrix}_{n-1 \times n-1}$$

$$+(-1)^{n+1}(1)det\begin{pmatrix} -1 & & \\ & \ddots & \\ & & -1 \end{pmatrix}$$

$$=(2-\lambda)P_{n-1}(\lambda)+(-1)^{n+1}(-1)^{n-1}$$

$$=(2-\lambda)P_{n-1}(\lambda)+1$$

$$=(2-\lambda)P_{n-2}(\lambda)+(-1)^{n-1+1}(-1)^{n-2})+1$$

$$=((2-\lambda)P_{n-2}+(2-\lambda)+1$$

$$\vdots$$

$$=(2-\lambda)^n+...+(2-\lambda)+1.\square$$

COROLLARY 5.2.3. *If n is odd and $n \geq 3$, then $3-\lambda$ is a factor of $P_{n-2}(\lambda)$.*

PROOF: By Proposition 5.2.2,

$$P_n(\lambda)=(2-\lambda)^n+...+(2-\lambda)+1$$

$$=(2-\lambda)^{n-1}[(2-\lambda)+1]+(2-\lambda)^{n-3}[(2-\lambda)+1]+...$$

$$+(2-\lambda)^2[(2-\lambda)+1]+[(2-\lambda)+1]$$

$$=(2-\lambda)^{n-1}(3-\lambda)+(2-\lambda)^{n-3}(3-\lambda)+...+(2-\lambda)(3-\lambda)+(3-\lambda)$$

$$=(3-\lambda)[(2-\lambda)^{n-1}+(2-\lambda)^{n-3}+...+(2-\lambda)+1].$$

Therefore, $(3-\lambda) \mid P_n(\lambda).\square$

PROPOSITION 5.2.4. *Let $\omega_1,\omega_2,\ldots,\omega_n$ be $(n+1)^{th}$ roots of unity with $\omega_i \neq 1$ for $i=1,\ldots,n$. The eigenvalues of $\mathbf{A}_\alpha$ are $2-\omega_1,2-\omega_2,\ldots,2-\omega_n$.*

PROOF: By Proposition 5.2.2, $P_n(\lambda)=0$ implies that $(2-\lambda)^n+(2-\lambda)^{n-1}+...+(2-\lambda)+1=0$. Since if $(2-\omega)-1 \neq 0$, $(2-\lambda)^n+(2-\lambda)^{n-1}+...+(2-\lambda)+1=(2-\lambda)^{n+1}-1=0$. Therefore, if $\lambda \neq 1$, then $(2-\lambda)^{n+1}=1$. Let $\omega_1,\ldots,\omega_n$ denote the $(n+1)^{th}$ roots of unity with $\omega_i \neq 1$, for all $i=1,\ldots,n$ we have $\lambda_1=2-\omega_1,\ldots,\lambda_n=2-\omega_n$. $\square$

PROPOSITION 5.2.5. *The eigenvectors* $v_1, v_2, ..., v_n$ *of* $\mathbf{A}_\alpha$ *are the following:*

$$v_i = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix},$$

where u_n *could be chosen as 1, and* $u_{n-1} = 1+(2-\lambda)$, $u_{n-2} = 1+(2-\lambda)+(2-\lambda)^2, ...,$ $u_1 = 1 + (2-\lambda) + ... + (2-\lambda)^{n-1}$, *for* $i = 1, ..., n$.

PROOF: For each eigenvalue λ_i, we assume that the eigenvector

$$v_i = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}.$$

and we have

$$\begin{pmatrix} 2 & 0 & 0 & \dots & 0 & 1 \\ -1 & 2 & 0 & \dots & 0 & 1 \\ 0 & -1 & 2 & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2 & 1 \\ 0 & 0 & 0 & \dots & -1 & 3 \end{pmatrix}_{n\times n} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_{n-1} \\ u_n \end{pmatrix} = \lambda_i \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_{n-1} \\ u_n \end{pmatrix},$$

which produces the following system of equations,

$$\begin{cases} 2u_1 + u_n & = \lambda_i u_1 \\ -u_1 + 2u_2 + u_n & = \lambda_i u_2 \\ -u_2 + 2u_3 + u_n & = \lambda_i u_3 \\ \quad \vdots & \\ -u_{n-2} + 2u_{n-1} + u_n & = \lambda_i u_{n-1} \\ -u_{n-1} + 3u_n & = \lambda_i u_n \end{cases}$$

Therefore,

$$\begin{cases} (2-\lambda)u_1 + u_n & = 0 \\ -u_1 + (2-\lambda)u_2 + u_n & = 0 \\ -u_2 + (2-\lambda)u_3 + u_n & = 0 \\ \quad \vdots & \\ -u_{n-2} + (2-\lambda)u_{n-1} + u_n & = 0 \\ -u_{n-1} + (3-\lambda)u_n & = 0 \end{cases}.$$

The solutions of this system of equations are

$$\begin{cases} u_1 & = [1 + (2-\lambda) + \ldots + (2-\lambda)^{n-1}]u_n \\ u_2 & = [1 + (2-\lambda) + \ldots + (2-\lambda)^{n-2}]u_n \\ \vdots & \\ u_{n-2} & = [1 + (2-\lambda) + (2-\lambda)^2]u_n \\ u_{n-1} & = [1 + (2-\lambda)]u_n. \end{cases}$$

Thus, if we choose $u_n = 1$, then

$$u_1 = 1 + (2-\lambda) + \ldots + (2-\lambda)^{n-1}$$

$$u_2 = 1 + (2-\lambda) + \ldots + (2-\lambda)^{n-2}$$

$$\vdots$$

$$u_{n-2} = 1 + (2-\lambda) + (2-\lambda)^2$$

$$u_{n-1} = 1 + (2-\lambda). \square$$

PROPOSITION 5.2.6. *The inverse of* $\mathbf{A}_\alpha$ *is* $\mathbf{A}_\alpha{}^{-1} = \frac{1}{q}(a_{ij})$, *where* $a_{ij} = 2^{n-i+j} - 2^{j-1}$ *if* $i \geq j$, $a_{ij} = 2^{j-1} + 2^{j-i-1}$ *if* $i < j$ *and* $q = det(\mathbf{A}_\alpha)$.

PROOF: Let

$$\mathbf{A}_\alpha = \begin{pmatrix} 2 & 0 & 0 & \dots & 0 & 1 \\ -1 & 2 & 0 & \dots & 0 & 1 \\ 0 & -1 & 2 & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2 & 1 \\ 0 & 0 & 0 & \dots & -1 & 3 \end{pmatrix}$$

and let

$$B = \frac{1}{q}\begin{pmatrix} 2^n-1 & -2+1 & -2^2+2 & \dots & -2^{n-2}+2^{n-3} & -2^{n-1}+2^{n-2} \\ 2^{n-1}-1 & 2^n-2 & -2^2+1 & \dots & -2^{n-2}+2^{n-4} & -2^{n-1}+2^{n-3} \\ 2^{n-2}-1 & 2^{n-1}-2 & 2^n-2^2 & \dots & -2^{n-2}+2^{n-5} & -2^{n-1}+2^{n-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 2^2-1 & 2^3-2 & 2^4-2^2 & \dots & 2^n-2^{n-2} & -2^{n-1}+1 \\ 2^1-1 & 2^2-2 & 2^3-2^2 & \dots & 2^{n-1}-2^{n-2} & 2^n-2^{n-1}. \end{pmatrix}$$

Let $C = \mathbf{A}_\alpha B$, $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. If $i > j$, then

$$\begin{aligned} c_{ij} &= a_{ii-1}b_{i-1j} + aiib_{ij} + a_{in}b_{nj} \\ &= \frac{1}{q}[(-1)(2^{n-(i-1)+j} - 2^{j-1}) + (2)(2^{n-i+j} - 2^{j-1}) + (1)(2^{n-n+j} - 2^{j-1})] \\ &= \frac{1}{q}(-2^{n-i+1+j} + 2^{j-1} + 2^{n-i+j+1} - 2^j + 2^j - 2^{j-1}) \\ &= 0. \end{aligned}$$

If $i < j$, then

$$\begin{aligned} c_{ij} &= \frac{1}{q}[(-1)(-2^{j-1} + 2^{j-(i-1)+1}) + (2)(-2^{j-1} + 2^{j-i-1}) + (1)(2^{n-n+j} - 2^{j-1})] \\ &= \frac{1}{q}(2^{j-1} - 2^{j-i} - 2^j + 2^{j-i} + 2^j - 2^{j-1}) \\ &= 0. \end{aligned}$$

If $i = j$, then

$$\begin{aligned} c_{ii} &= a_{ii-1}b_{i-1i} + a_{ii}b_{ii} + a_{in}b_{ni} \\ &= \frac{1}{q}[(-1)(-2^{i-1} + 2^{i-(i-1)-1}) + (2)(2^n - 2^{i-1}) + (1)(2^{n-n+i} - 2^{i-1})] \\ &= \frac{1}{q}(2^{i-1} - 1 + 2^{n+1} - 2^i + 2^i - 2^{i-1}) \\ &= \frac{2^{n+1} - 1}{q} = 1. \end{aligned}$$

Therefore, $C = I$, which is the identity matrix. If we let $D = B\mathbf{A}_\alpha$, by the similar calculation, we get $D = I$. Thus, we have $\mathbf{A}_\alpha B = B\mathbf{A}_\alpha = I$, i.e., $B = {\mathbf{A}_\alpha}^{-1}$. □

PROPOSITION 5.2.7. $\mathbf{A}_\alpha = LU$, *where* $L = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ -\frac{1}{2} & 1 & 0 & \dots & 0 & 0 \\ 0 & -\frac{1}{2} & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & -\frac{1}{2} & 1 \end{pmatrix}$ *and*

$$U = \begin{pmatrix} 2 & 0 & \dots & 0 & 1 \\ 0 & 2 & \dots & 0 & 1 + \frac{1}{2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 2 & 1 + \frac{1}{2} + \dots + (\frac{1}{2})^{n-1} \\ 0 & 0 & \dots & 0 & 3 + \frac{1}{2} + \dots + (\frac{1}{2})^{n-1} + (\frac{1}{2})^n \end{pmatrix}.$$

PROOF: Trivial. □

CHAPTER 6

IMAGE ALGEBRA IN HEXAGONAL LATTICE

In this chapter, we present some results concerning the decomposition and invertibility of circulant templates over the hexagonal sampled images under the generalized convolution operation ($\oplus$) of image algebra [23]. Many of the results are due to D. Lucas and L. Gibson [19]. Two types of polynomial representation for hexagonal images are also discussed.

§6.1. A Brief Review of the Image Algebra

In this section, a brief review of the fundamental concepts and notation of the image algebra will be given.

The image algebra is an heterogeneous algebra structure specially designed for image processing [23]. It has been demonstrated that many commonly used image processing transformations, such as generalized convolutions, Discrete Fourier Transform, edge detectors, and morphological operations, can be easily expressed in terms of the image algebra.

An image algebra is an algebra whose operands are images and subimages (or neighborhoods). It deals with six basic type of operands, namely, value sets, point sets, the elements of the value sets and point sets, images, and templates.

A *value set* can be any semi-group. The most commonly used value sets in image processing are the set of positive integers, integers, rational numbers, real

numbers, positive real numbers, or complex numbers. These sets will be denoted by $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$, $\mathbb{R}^+$, $\mathbb{C}$, respectively. The value set will be denoted by $\mathbf{F}$.

A *a point set* is a topological space, in particular a subset of an n-dimensional Euclidean space, $\mathbb{R}^n$, for some n. Point sets are commonly denoted by the symbols $\mathbf{X}$ and $\mathbf{Y}$. The elements of such sets are denoted by lower case letters. Familiar point sets include the rectangular and hexagonal arrays.

DEFINITION 6.1.1. *Let* $\mathbf{X}$*, and* $\mathbf{F}$ *be a point set and a value set, respectively. An* $\mathbf{F}$ *valued image* $\mathbf{a}$ *on* $\mathbf{X}$ *is a function* $\mathbf{a}$*:* $\mathbf{X} \to \mathbf{F}$.

Thus, the graph of an $\mathbf{F}$ valued image $\mathbf{a}$ on $\mathbf{X}$ is of the form

$$\mathbf{a} = \{(\mathbf{x}, \mathbf{a}(\mathbf{x})) : \mathbf{a}(\mathbf{x}) \in \mathbf{F}, \text{ for all } \mathbf{x} \in \mathbf{X}\}.$$

The set $\mathbf{X}$ is called the *set of image coordinates* of $\mathbf{a}$, and the range of the function $\mathbf{a}$ is called the *set of image values* of $\mathbf{a}$. The pair $(\mathbf{x}, \mathbf{a}(\mathbf{x}))$ is called a *picture element* or a *pixel,* $\mathbf{x}$ the *pixel location,* and $\mathbf{a}(\mathbf{x})$ the *pixel* (or *gray*) *value.* We will denote the set of all $\mathbf{F}$ valued images on $\mathbf{X}$ by $\mathbf{F}^{\mathbf{X}}$. We make no distinction between an image and its graph.

DEFINITION 6.1.2. *An image* $\mathbf{a}$*:* $\mathbf{X} \to \mathbf{F}$ *has finite support on* $\mathbf{X}$ *if* $\mathbf{a}(\mathbf{x}) \neq 0$ *for only a finite number of elements* $\mathbf{x} \in \mathbf{X}$.

Another basic, but very powerful tool of the image algebra, is the generalized template.

DEFINITION 6.1.3. *Let* $\mathbf{X}$ *and* $\mathbf{Y}$ *be two coordinate sets, and let* $\mathbf{F}$ *be a value set. A generalized* $\mathbf{F}$ *valued template* $\mathbf{t}$ *from* $\mathbf{Y}$ *to* $\mathbf{X}$ *is a function* $\mathbf{t}$*:* $\mathbf{Y} \to \mathbf{F}^{\mathbf{X}}$.

Thus, for each $\mathbf{y} \in \mathbf{Y}$, $\mathbf{t}(\mathbf{y}) \in \mathbf{F}^{\mathbf{X}}$, or equivalently, $\mathbf{t}(\mathbf{y})$ is an $\mathbf{F}$-valued image on $\mathbf{X}$. For notational convenience, we define $\mathbf{t_y} \equiv \mathbf{t}(\mathbf{y})$. Thus,

$$\mathbf{t_y} = \{(\mathbf{x}, \mathbf{t_y}(\mathbf{x})) : \mathbf{x} \in \mathbf{X}\}.$$

The sets $\mathbf{Y}$ and $\mathbf{X}$ are called the *domain* and *range space* of $\mathbf{t}$, respectively. The point $\mathbf{y}$ is called the *domain* point of the template $\mathbf{t}$, and the values $\mathbf{t_y}(\mathbf{x})$ are called the *weights* of the template $\mathbf{t}$ at $\mathbf{y}$. Note that the set of all $\mathbf{F}$-valued templates from $\mathbf{Y}$ to $\mathbf{X}$ can be denoted by $(\mathbf{F}^{\mathbf{X}})^{\mathbf{Y}}$.

If $\mathbf{t}$ is a template from $\mathbf{Y}$ to $\mathbf{X}$, then the set

$$\mathbf{S}(\mathbf{t_y}) = \{\mathbf{x} \in \mathbf{X} : \mathbf{t_y}(\mathbf{x}) \neq 0\}$$

is called the *support* of $\mathbf{t_y}$.

If $\mathbf{t}$ is an $\mathbf{F}$ valued template from $\mathbf{X}$ to $\mathbf{X}$, and $\mathbf{X}$ is a subset of $\mathbb{R}^n$, then $\mathbf{t}$ is called *translation invariant* (or *shift-invariant*) if and only if for each triple $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$, with $\mathbf{x} + \mathbf{z}$ and $\mathbf{y} + \mathbf{z} \in \mathbf{X}$, we have that

$$\mathbf{t_y}(\mathbf{x}) = \mathbf{t_{y+z}}(\mathbf{x} + \mathbf{z}).$$

Note that a translation invariant template must be an element of $(\mathbf{F}^{\mathbf{X}})^{\mathbf{X}}$. Invariant operators on $\mathbb{Z} \times \mathbb{Z}$ are commonly expressed in terms of polynomials of two variables. A template which is not necessarily translation invariant is called *translation variant* or, simply, a *variant template*. Translation invariant templates occur naturally in digital image processing.

The basic operations on and between $\mathbf{F}$ valued images are naturally derived from the algebraic structure of the value set $\mathbf{F}$.

Let $\mathbf{X}$ be a subset of $\mathbf{R}^n$. Suppose $\mathbf{a} \in \mathbf{R}^{\mathbf{X}}$ and $\mathbf{t} \in (\mathbf{R}^{\mathbf{X}})^{\mathbf{X}}$.

Addition on images is defined as follows: If $\mathbf{a}, \mathbf{b} \in \mathbf{F}^{\mathbf{X}}$, then

$$\mathbf{a} + \mathbf{b} \equiv \{(\mathbf{x}, \mathbf{c}(\mathbf{x})) : \mathbf{c}(\mathbf{x}) = \mathbf{a}(\mathbf{x}) + \mathbf{b}(\mathbf{x}), \mathbf{x} \in \mathbf{X}\}.$$

Higher level operations are the ones that involve operations between templates and images, and between templates only.

The addition of two templates is defined pointwise. If $\mathbf{s}$ and $\mathbf{t} \in (\mathbf{R}^{\mathbf{X}})^{\mathbf{X}}$, then we have

$$(\mathbf{s} + \mathbf{t})_{\mathbf{y}}(\mathbf{x}) = \mathbf{s}_{\mathbf{y}}(\mathbf{x}) + \mathbf{t}_{\mathbf{y}}(\mathbf{x}).$$

DEFINITION 6.1.4. *The generalized convolution of an image* $\mathbf{a}$ *together with a template* $\mathbf{t}$ *is defined by*

$$\mathbf{a} \oplus \mathbf{t} = \{(\mathbf{y}, \mathbf{b}(\mathbf{y})) : \mathbf{b}(\mathbf{y}) = \sum_{\mathbf{x} \in \mathbf{X}} \mathbf{a}(\mathbf{x}) \mathbf{t}_{\mathbf{y}}(\mathbf{x}), \mathbf{y} \in \mathbf{X}\}.$$

Linear convolution plays a fundamental role in image processing. It is involved in such important examples as the Discrete Fourier Transform, the Laplacian, the mean or average filter and the Gaussian mean filter.

DEFINITION 6.1.5. *If* $\mathbf{s}$ *and* $\mathbf{t}$ *are templates on* $\mathbf{X}$*, then we define the generalized convolution of the two templates as the template* $\mathbf{r} = \mathbf{s} \oplus \mathbf{t}$ *by defining each image function* $\mathbf{r}_{\mathbf{y}}$ *by the rule*

$$\mathbf{r}_{\mathbf{y}} = \{(\mathbf{z}, \mathbf{r}_{\mathbf{y}}(\mathbf{z})) : \mathbf{r}_{\mathbf{y}}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbf{X}} \mathbf{t}_{\mathbf{y}}(\mathbf{x}) \mathbf{s}_{\mathbf{x}}(\mathbf{z}), \text{ where } \mathbf{z} \in \mathbf{X}\}.$$

Note that $\mathbf{r}$ can be viewed as a generalization of the usual notion of the composition of two convolution operators. If the templates $\mathbf{s}$ and $\mathbf{t}$ are translation invariant,

then, except for values near the boundary, the previous definition agrees with the usual definition of polynomial product.

Note also that if $\mathbf{s}$ and $\mathbf{t}$ are two invariant templates, then $\mathbf{r}$ would be an invariant template too. Computing $\mathbf{r}$ at just any one $\mathbf{y} \in \mathbf{Y}$ is sufficient to define the template everywhere.

Many other image operations are described in detail in Ritter et. al. [23]. A precise investigation of the linear convolution can also be found in Gader [5], and an extensive study of other non-linear template operations can be found in Davidson [3], Li [14] and Manseur [20].

If $\mathbf{X}$ is a finite rectangular subset of the plane with m rows and n columns, then it can be linearly ordered left to right and row by row. Thus, we can write $\mathbf{X} = \{\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_{mn}\}$.

Let $(M_{mn}, +, *)$ denote the ring of $mn \times mn$ matrices with entries from $\mathbf{F}$ under matrix addition and multiplication. For any template $\mathbf{t}$, we define a matrix $M_{\mathbf{t}} = (m_{ij})$ where $m_{ij} = \mathbf{t}_{\mathbf{x}_j}(\mathbf{x}_i)$. For the sake of notational convenience we will write $\mathbf{t}_{ij}$ for $\mathbf{t}_{\mathbf{x}_j}(\mathbf{x}_i)$.

Define the mapping $\phi : (\mathbf{F}^{\mathbf{X}})^{\mathbf{X}} \to M_{mn}$ by $\phi(\mathbf{t}) = M_{\mathbf{t}}$.

The next Theorem was proved by Ritter and Gader [5]. It shows that there is an embedding of the linear algebra in the image algebra.

THEOREM 6.1.6. *The mapping ϕ is an isomorphism from the ring $((\mathbf{F}^{\mathbf{X}})^{\mathbf{X}}, +, \oplus)$ onto the ring $(M_{mn}, +, *)$. That is, if $\mathbf{s}, \mathbf{t} \in (\mathbf{F}^{\mathbf{X}})^{\mathbf{X}}$, then*

(1) $\phi(\mathbf{s} + \mathbf{t}) = \phi(\mathbf{s}) + \phi(\mathbf{t})$ *or* $M_{\mathbf{s}+\mathbf{t}} = M_{\mathbf{s}} + M_{\mathbf{t}}$

(2) $\phi(\mathbf{s} \oplus \mathbf{t}) = \phi(\mathbf{s})\phi(\mathbf{t})$ *or* $M_{\mathbf{s}\oplus\mathbf{t}} = M_{\mathbf{s}} M_{\mathbf{t}}$

(3) ϕ *is one-to-one and onto.*

This theorem clearly states that template inversion or deconvolution is equivalent to matrix inversion. Actually, a more powerful implication of this theorem is that any tool available in linear algebra is directly applicable to any problem in the image algebra.

DEFINITION 6.1.7. *Let* $\mathbf{X}$ *be an* $m \times n$ *rectangular point set. We say that the mapping* $\psi : \mathbf{X} \to \mathbf{X}$ *is a circulant translation if and only if* ψ *is of the form* $\psi(\mathbf{x}) = (\mathbf{x} + \mathbf{y}) \mod (m, n)$, *for some* $\mathbf{y} \in \mathbf{X}$.

DEFINITION 6.1.8. *We say that* $\mathbf{t} \in (\mathbf{F}^{\mathbf{X}})^{\mathbf{X}}$ *is circulant if and only if for every circulant translation* ψ, *the equation* $\mathbf{t}_{\mathbf{x}}(\mathbf{y}) = \mathbf{t}_{\psi(\mathbf{x})}(\psi(\mathbf{y}))$ *holds.*

Remark: This last definition shows that a circulant template is completely determined if it is defined at only one point.

§6.2. Hexagonal Images and Polynomial Rings

The point set $\mathbf{X}$ for hexagonal arrays based on the level k $\mathbf{GBT}_2$ address is the quotient ring $\mathbf{GBT}_2/I'_k$ as indicated in Section 2.3. We use A_k to denote the ring $\mathbf{GBT}_2/I'_k$ in this Section. A function $\mathbf{a}$ from A_k to the real numbers $\mathbf{R}$ is an image as defined in Section 6.1, Since we have the one-to-one correspondence between A_k and the hexagons in the level k aggregate, for each $\mathbf{GBT}_2$ address v, $\mathbf{a}(v)$ is the pixel value of the hexagon grid [19].

The set $\mathbf{F}^{A_k}$ of images on a level k aggregate is itself a ring in two distinct ways. The first is pointwise. Given two images $\mathbf{a}$ and $\mathbf{b}$, one can define

$$(\mathbf{a} + \mathbf{b})(v) = \mathbf{a}(v) + \mathbf{b}(v)$$

and

$$(\mathbf{a} * \mathbf{b})(v) = \mathbf{a}(v) \times \mathbf{b}(v)$$

for all v in A_k. These operations result in a commutative ring structure on $\mathbf{F}^{A_k}$. The other ring structure on $\mathbf{F}^{A_k}$ is a convolution ring. Addition in this ring is pointwise as above. Multiplication is convolution, defined by

$$(\mathbf{a} * \mathbf{b})(v) = conv(\mathbf{a}, \mathbf{b})(v) = \sum_{\omega \in A_k} \mathbf{a}(\omega)\mathbf{b}(v - \omega)$$

where $v - \omega$ is an operation in A_k. This means that as pixels from the image move across the boundary of the image $\mathbf{a}$ they wrap around and reenter $\mathbf{a}$ from the other side.

Let $\eta(1) = 1$ in A_k. Define the function $\eta : \mathbf{Z}/(7^k) \mapsto A_k$ by $\eta(i) = \underbrace{\eta(1) + \cdots + \eta(1)}_{i}$, the sum of i $1's$ in A_k. Thus, in A_2, $\eta(0) = 0$, $\eta(1) = 1$, $\eta(2) = 12$, $\eta(3) = 13$, $\eta(4) = 44$, etc.

With each image $\mathbf{a}$ in A_k, one can associate a polynomial $f_{\mathbf{a}}(x)$ defined by

$$f_{\mathbf{a}}(x) = \sum_{v \in A_k} \mathbf{a}(v)x^{\xi(v)}$$

where $\xi = \eta^{-1}$ is the isomorphism from A_k to $\mathbf{Z}/(7^k)$. For two images $\mathbf{a}$ and $\mathbf{b}$ we have

$$f_{\mathbf{a}}(x) * f_{\mathbf{b}}(x) = \sum_{v \in A_k} \mathbf{c}(v)x^{\xi(v)}, \text{ where}$$

$$\mathbf{c}(v) = \sum_{w \in A_k} \mathbf{a}(w)\mathbf{b}(v - w), \text{ the convolution of } \mathbf{a} \text{ and } \mathbf{b}.$$

This last equality results from the fact that

$$\mathbf{a}(w)x^{\xi(w)} * \mathbf{b}(v - w)x^{\xi(v-w)} = \mathbf{a}(w)\mathbf{b}(v - w)x^{\xi(v)} \text{ for all } w \in A_k.$$

Addition of polynomials likewise corresponds to image addition. Therefore, the set of images on A_k with the convolution ring structure is isomorphic to the quotient ring of polynomials with exponents taken modulo 7^k.

§6.3. $\mathbf{GBT_2}$ Circulant Templates

In general, an $\mathbf{F}$ valued template $\mathbf{t}$ on a level k $\mathbf{GBT_2}$ aggregate A_k is a mapping from an index set $\mathbf{Y}$ to the set of functions from A_k to $\mathbf{F}$. The generalized convolution between a level k $\mathbf{GBT_2}$ image and a template $\mathbf{t}$ can be considered as the image convolution. Especially, the template $\mathbf{t}$ is a *circulant template* since the ring structure on A_k causes cells which cross the aggregate boundary to reenter the aggregate at another location [19].

In Section 6.2, we saw that image convolution is equivalent to polynomial multiplication in the quotient ring of polynomials whose exponents are taken modulo 7^k. In this ring

$$x^{7^k} = x^0 = 1$$

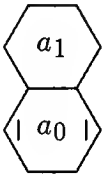
and each ring element is uniquely represented by a polynomial of degree less than 7^k. Therefore questions concerning the decomposition or invertibility of a circulant template under the circle plus operation can be posed as questions about the corresponding polynomials.

The next Theorem was proved by D. Lucas and L. Gibson [19].

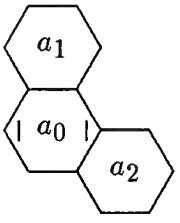
THEOREM 6.3.1. *A circulant template is invertible if and only if each of its linear factors is invertible.*

PROOF: The Fundamental Theorem of Algebra states that any polynomial with real or complex coefficients can be factored into linear factors in the field of complex numbers. The template corresponding to a linear factor $(x - r)$ has a *one* at $\mathbf{GBT_2}$ address 1 and $-r$ at $\mathbf{GBT_2}$ address 0. It follows that any circulant template on A_k can be written as a $\oplus$ of these simple templates. Therefore, a circulant template is invertible if and only if all of these simple templates are invertible. □

COROLLARY 6.3.2. *Any template in first level aggregate can be decomposed into the* $\oplus$ *of the templates with the shape*

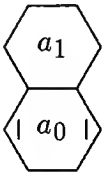


and with the shape

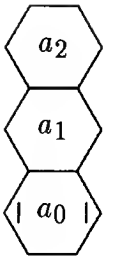


where $a_i \in \mathbb{R}$.

Any template in second or higher level aggregates can be decomposed into the $\oplus$ *of the templates with the shape*



and the templates with the shape



The next theorem was also proved by D. Lucas and L. Gibson.

THEOREM 6.3.3. *Any circulant template in a* $\mathbf{GBT_2}$ *level* k *aggregate is invertible if and only if none of the roots of its corresponding polynomial are* $(7^k)^{th}$ *roots of one.*

PROOF: We can derive this characterization of invertibility for circulant templates by defining

$$\mathbf{t}_r(x) = \sum_{n=1}^{7^k} r^{n-1} x^{7^K - n}.$$

By multiplying $\mathbf{t}_r(x)$ by $(x - r)$ one sees that

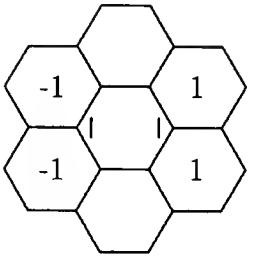
$$(x - r) * \mathbf{t}_r(x) = x^{7^k} - r^{7^k} = 1 - r^{7^k}.$$

Therefore, if r^{7^k} is not equal to 1, then the polynomial

$$\mathbf{t}_r(x)/(1 - r^{7^k})$$

is the inverse of $(x - r)$. Otherwise $(x - r)$ is a zero divisor and not invertible. □

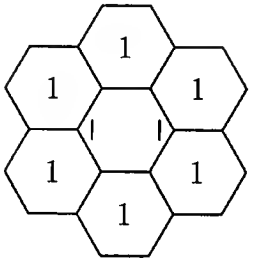
Using level one aggregate as an example, the template



has for its corresponding polynomial

$$-x^5 - x^4 + x^3 + x^2 = -x^2(x-1)(x+1)^2$$

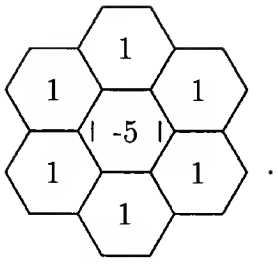
one of whose roots is 1. Thus, it is not invertible. But the template



has polynomial

$$x^6 + x^5 + x^4 + x^3 + x^2 + x = x(x+1)(x^2+x+1)(x^2-x+1)$$

and is invertible since the roots of the last two quadratics are the cube and sixth roots of 1 respectively. In fact, its inverse template is one sixth of the integer template



§6.4. Another Representation of $\mathbf{GBT}_2$ Circulant Templates

The family of real valued circulant templates on $n \times m$ rectangular images is isomorphic to a quotient ring of the ring of real polynomials in two variables.

We can define a polynomial for hexagonal sampled images in a similar way.

As shown in Figure 8, if r is the dimension of a side of one of the six equilateral triangles that make up a basic hexagon (the hexagon radius) and r is chosen as 2, then we can construct the polynomial

$$p(x,y) = a_{00}(x^3)^0(y^{\sqrt{3}})^0 + a_{02}(x^3)^0(y^{\sqrt{3}})^2 + a_{0-2}(x^3)^0(y^{\sqrt{3}})^{-2} + a_{11}(x^3)^1(h^{\sqrt{3}})^1 +$$

$$a_{1-1}(x^3)^1(y^{\sqrt{3}})^{-1} + a_{-11}(x^3)^{-1}(y^{\sqrt{3}})^1 + a_{-1-1}(x^3)^{-1}(y^{\sqrt{3}})^{-1},$$

according to the center of the hexagons.

If we let $u = x^3$ and $v = y^{\sqrt{3}}$, then

$$p(x,y) = q(u,v) = a_{00} + a_{02}v^2 + a_{0-2}v^{-2} + a_{11}uv + a_{1-1}uv^{-1} + a_{-11}u^{-1}v + a_{-1-1}u^{-1}v^{-1}.$$

Notice that for each term $u^m v^n$ of the polynomial $q(u,v)$, we have m and n are either both odd or both even.

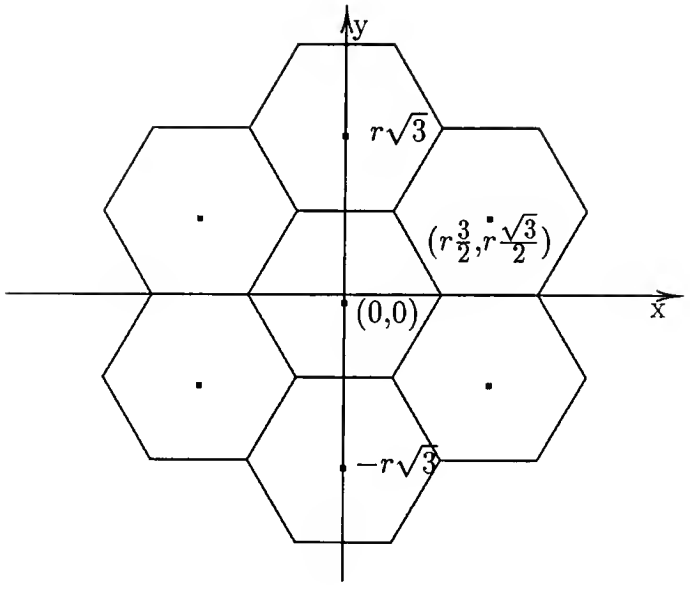
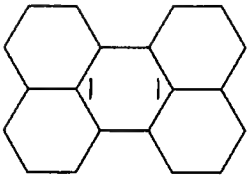


Figure 8: First level aggregate over the Cartesian Plane.

For the polynomial $q(u, v)$, we can set up a 5×5 matrix as follow:

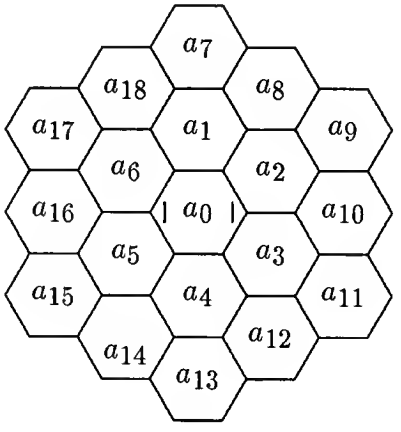
$$\begin{pmatrix} 0 & 0 & a_{0-2} & 0 & 0 \\ 0 & a_{-1-1} & 0 & a_{1-1} & 0 \\ 0 & 0 & a_{00} & 0 & 0 \\ 0 & a_{-11} & 0 & a_{11} & 0 \\ 0 & 0 & a_{02} & 0 & 0 \end{pmatrix}.$$

Manseur [20] discussed the decomposition of polynomial with 2 variables. For a size 5×5 template $\mathbf{t}$, she proved that $\mathbf{t} = \mathbf{t}_1\mathbf{t}_2 + \mathbf{t}_3\mathbf{t}_4 + \mathbf{t}_5$, where $\mathbf{t}_1, \mathbf{t}_2, \mathbf{t}_3, \mathbf{t}_4$ and $\mathbf{t}_5$ are size 3×3 templates. This decomposition method does not work well for hexagonally sampled templates since after the decomposition, a size 3×3 template corresponds the template with the shape



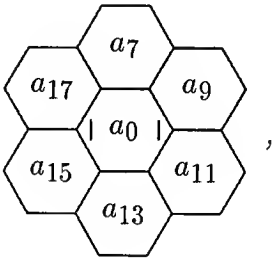
which does not provide the smaller template as we wanted.

PROPOSITION 6.4.1. *If the template*

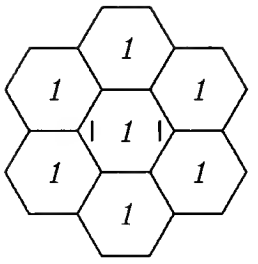
$\mathbf{t} =$ 

,

where $a_i \in \mathbb{R}$, *for* $i = 0, 1, \ldots, 18$, *and* $a_8 = a_7 + a_9, a_{10} = a_9 + a_{11}, a_{12} = a_{11} + a_{13}$, $a_{14} = a_{13} + a_{15}, a_{16} = a_{15} + a_{17}, a_{18} = a_{17} + a_7$, *then,* $\mathbf{t} = \mathbf{s}_1 \oplus \mathbf{s}_2 + \mathbf{r}$, *where*

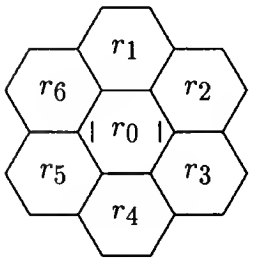
$\mathbf{s}_1 =$ 

,

$\mathbf{s}_2 =$ 

,

and

$\mathbf{r} =$ 

,

where $r_0 = -a_7 - a_9 - a_{11} - a_{13} - a_{15} - a_{17}$, $r_1 = a_1 - a_0 - a_7 - a_9 - a_{17}$, $r_2 = a_2 - a_0 - a_7 - a_9 - a_{11}$, $r_3 = a_3 - a_0 - a_9 - a_{11} - a_{13}$, $r_4 = a_4 - a_0 - a_{11} - a_{13} - a_{15}$, $r_5 = a_5 - a_0 - a_{13} - a_{15} - a_{17}$, $r_6 = a_6 - a_0 - a_{15} - a_{17} - a_7$.

PROOF: The polynomials correspond to the templates $\mathbf{s}_1$ and $\mathbf{s}_2$ are

$$s_1(u,v) = a_0 + a_7v^2 + a_9uv + a_{11}uv^{-1} + a_{13}v^{-2} + a_{15}u^{-1}v^{-1} + a_{17}u^{-1}v,$$

and

$$s_2(u,v) = 1 + v^2 + uv + uv^{-1} + v^{-2} + u^{-1}v^{-1} + u^{-1}v,$$

respectively. Therefore,

$$\begin{aligned} s_1(u,v)s_2(u,v) = {} & (a_0 + a_7 + a_9 + a_{11} + a_{13} + a_{15} + a_{17}) + \\ & + (a_0 + a_7 + a_9 + a_{17})v^2 + (a_0 + a_7 + a_9 + a_{11})uv + \\ & + (a_0 + a_9 + a_{11} + a_{13})uv^{-1} + (a_0 + a_{11} + a_{13} + a_{15})v^{-2} + \\ & + (a_0 + a_{13} + a_{15} + a_{17})u^{-1}v^{-1} + (a_0 + a_{15} + a_{17} + a_7)u^{-1}v + \\ & + a_7v^4 + (a_7 + a_9)uv^3 + a_9u^2v^2 + \\ & + (a_9 + a_{11})u^2 + a_{11}u^2v^{-2} + (a_{11} + a_{13})uv^{-3} + \\ & + a_{13}v^{-4} + (a_{13} + a_{15})u^{-1}v^{-3} + a_{15}u^{-2}v^{-2} + \\ & + (a_{15} + a_{17})u^{-2} + a_{17}u^{-2}v^2 + (a_{17} + a_7)u^{-1}v^3. \end{aligned}$$

The polynomial corresponds to the template **r** is

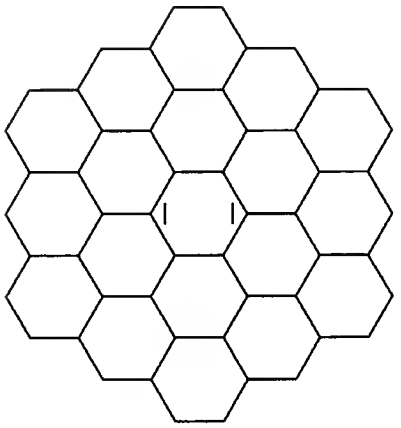
$$\begin{aligned} r(u,v) = {} & (-a_7 - a_9 - a_{11} - a_{13} - a_{15}) + \\ & + (a_1 - a_0 - a_7 - a_9 - a_{17})v^2 + (a_2 - a_0 - a_7 - a_9 - a_{11})uv + \\ & + (a_3 - a_0 - a_9 - a_{11} - a_{13})uv^{-1} + (a_4 - a_0 - a_{11} - a_{13} - a_{15})v^{-2} + \\ & + (a_5 - a_0 - a_{13} - a_{15} - a_{17})u^{-1}v^{-1} + (a_6 - a_0 - a_{15} - a_{17} - a_7)u^{-1}v. \end{aligned}$$

Therefore, $s_1(u,v)s_2(u,v) + r(u,v) = t(u,v)$, where

$$\begin{aligned} t(u,v) = {} & a_0 + a_1v^2 + a_2uv + a_3uv^{-1} + a_4v^{-2} + a_5u^{-1}v^{-1} + a_6u^{-1}v + \\ & + a_7v^4 + a_8uv^3 + a_9u^2v^2 + a_{10}u^2 + a_{11}u^2v^{-2} + a_{12}uv^{-3} + \\ & + a_{13}v^{-4} + a_{14}u^{-1}v^{-3} + a_{15}u^{-2}v^{-2} + a_{16}u^{-2} + a_{17}u^{-2}v^2 + a_{18}u^{-1}v^3, \end{aligned}$$

and $t(u,v)$ is the polynomial of the template **t**. □

The author is still working on the decomposition of a template with the shape



and arbitrary gray values into $\mathbf{s}_1 \oplus \mathbf{s}_2 + \mathbf{s}_3$, where $\mathbf{s}_i$'s are templates with a first level aggregate shape.

The question raised here is that whether we can decompose a template $\mathbf{t}$ with a second level aggregate shape (See Figure 2) into the form $\mathbf{s}_1 \oplus \mathbf{s}_2 \oplus \mathbf{s}_3 \oplus \mathbf{s}_4 + \mathbf{s}_5$, where $\mathbf{s}_i$'s are the templates with a first level aggregate shape. Obviously, if we convolute a template with a first level shape 4 times, we can not get the template with a second level aggregate shape. The author is presently working to determine the possible decompositions of $\mathbf{t}$.

CHAPTER 7

FINAL REMARKS

This dissertation is not of the sort where some conclusion can be drawn. In short summary, the focal result of the dissertation was the proof that $\mathbf{EGBT}_n$ is isomorphic as a ring to the $(2^{n+1}-1)$-adic integers if $n+1$ and $2^{n+1}-1$ are relatively prime. This naturally leads to the question of whether $\mathbf{EGBT}_n$ and the $(2^{n+1}-1)$-adic integers are isomorphic if $n+1$ and $2^{n+1}-1$ are not relatively prime. The author hopes to investigate this question at a later date.

REFERENCES

1. N. Ahuja, *On approaches to polygonal decomposition for hierarchical image representation*, Computer Vision, Graphics Image Processing **24** (November, 1983), 200–214.

2. Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.

3. J. L. Davidson, *Lattice Structure in the Image Algebra and their Applications*, Ph.D. Dissertation, University of Florida, Gainesville, FL (1989).

4. L. Fuchs, "Infinite Abelian Groups I," Academic Press, New York, 1970, p. 62.

5. P. D. Gader, *Image Algebra Techniques for Parallel Computation of Discrete Fourier Transforms and General Linear Transforms*, Ph.D. Dissertation, University of Florida, Gainesville, Fl (1986).

6. L. Gibson and D. Lucas, *Spatial data processing using Generalized Balanced Ternary*, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (June, 1982), 566–571.

7. L. Gibson and D. Lucas, *Vectorization of raster images using hierarchical methods*, Computer Graphics and Image Processing **20** (1982), 82–89.

8. L. Gibson and D. Lucas, *Pyramid algorithms for automated target recognition*, Proceedings of the IEEE National Aerospace and Electronics Conference - NAECON, Dayton, Ohio, (1986), 215–219.

9. M. J. E. Golay, *Hexagonal Parallel Pattern Transformations*, IEEE Trans. Comput. **vol. C-18** (Aug. 1969), 733–740.

10. N. Jacobson, "Basic Algebra II," W. H. Freeman and Company, San Francisco, 1980, p. 74.

11. I. Kaplansky, "Infinite Abelian Groups," University of Michigan Press, Ann Arbor, 1956, p. 43.

12. W. Z. Kitto, A. Vince and D. C. Wilson, *An Isomorphism Between the p-adic Integers and a Ring Associated with a Tiling of N-space by Permutohedra* , submitted.

13. Neal Koblitz, "*p*-adic Numbers, *p*-adic Analysis, and Zeta-Functions," Springer Verlag, New York, 1977.

14. D. Li, *Recursive Operations in Image Algebra and their Applications to Image Processing*, Ph.D. Dissertation, University of Florida, Gainesville, Fl (1990).

15. D. Lucas, *A Multiplication in N-Space*, Proc. Amer. Math. Soc. **74** (1979), 1–8.

16. D. Lucas, Personal Communication.

17. D. Lucas and L. Gibson, *Image pyramids and partitions*, Seventh International Conference on Pattern Recognition, Montreal, Canada, **1** (1984), 230–233.

18. D. Lucas and L. Gibson, *Techniques to exploit the relation between polynomial representations and moments of pictures*, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, San Francisco, CA (1985), 138–143.

19. D. Lucas and Laurie Gibson, *Template decomposition and inversion over hexagonally sampled images*, Proceedings of the 1991 SPIE Image Algebra and Morphological Image Processing II, San Diego, CA (1991), 157–163.

20. Z. Z. Manseur, *Decomposition and Inversion of Convolution Operators*, Ph.D. Dissertation, University of Florida, Gainesville, FL (1990).

21. B. H. McCormick, *The Illinois pattern recognition computer - ILLIAC III*, IEEE Trans. Electron. Comput. **vol. EC-12** (Dec. 1963), 791–813.

22. K. Preston, *Feature Extraction by Golay Hexagonal Pattern Transforms*, IEEE Trans. Comput. **vol. C-20** (Sept. 1971), 1007–1014.

23. G. X. Ritter, J. N. Wilson and J. L. Davidson, *Image Algebra: An Overview*, Journal of Computer Vision, Graphics and Image Processing **49** (1990), 297–331.

24. D. K. Scholten and S. G. Wilson, *Chain coding with a hexagonal lattice*, IEEE Tran. on Pattern Analysis and Machine Intelligence (September, 1983), 526–533.

25. J. Serra, "Image Analysis and Mathematical Morphology," Academic Press, San Diego, 1988, pp. 257–296.

26. Jean-Pierre Serre, "A Course in Arithmetic," Springer Verlag, New York, 1973.

27. L. F. Toth, "Regular Figures," Pergamon Press, New York, 1964, p. 110.

28. A. Vince, *Aggregate Tessellations*, submitted.

BIOGRAPHICAL SKETCH

Wei Zhang Kitto was born on July 8, 1955, in Beijing, China. She received a bachelor's degree in mathematics from East China Institute of Textile Science and Technology in 1982, and a master's degree in mathematics from University of Florida in 1986. Her research interests include applied mathematics, image processing, and computer vision.

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

David C. Wilson

David C. Wilson, Chairman
Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

Gerhard Ritter

Gerhard X. Ritter, Cochairman
Professor of Computer and
Information Sciences

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

Andrew Vince
Associate Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

Li-Chien Shen
Associate Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

Arun K. Varma
Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

Joseph N. Wilson
Assistant Professor of Computer and Information Sciences

This dissertation is submitted to the Graduate Faculty of the Department of Mathematics in the College of Liberal Arts and Sciences and to the Graduate School and was accepted as partial fulfillment of the requirements for the degree of Doctor of Philosophy.

December, 1991

Dean, Graduate School